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 2021, 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) 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

6. Electronic Communications
    - Email
    - School website
    - Cloud platforms
    - Digital images and videos

7. Social Media
    - Staff, pupils and parents social media presence

8. 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

A1: KS1 Online Acceptable Use Agreement (Pupils)
A2: KS2 Online Acceptable Use Agreement (Pupils)
A3: ER/R Online Acceptable Use Agreement (Pupils)
A4: Staff and Governors: Acceptable Use Agreement
A5: Guidance for Parents, Visitors & Contractors
A6: Handling a sexting / nude selfie incident
A7: How specific infringements will be handled – Sanctions etc.
A8: Template for conversations (verbally on via email) for under age viewing/gameplay

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out key principles and expectations for all members of the school community at LCS with respect to their online behaviour, attitudes and activities, and the use of IT-based technologies (including when devices are offline).
- Safeguard and protect the children and staff.
- Facilitate the safe, responsible and respectful use of technology to support teaching & 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.
- 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.

- Establish 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).

Risks

We aim to minimise risk at all times. Annex D Online Safety (from KSCIE 2021) summarises risks under three different categories. This is reflected in the main areas of risk we have listed for our school community below:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and wellbeing (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of the LCS community (including staff, pupils, volunteers, parents/carers, visitors, contractors, community users) who have access to and are users of LCS IT systems and digital devices, both in and out of LCS.

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 Configurator/Mosyle management
- Chromebooks – managed through Google Admin
- Smart phones with email, web functionality, managed through Apple Configurator/Mosyle management
- iPod touches with email, web functionality, managed through Apple Configurator/Mosyle management
- Desktop PCS with web functionality – managed by our technician
- Lego WeDo Robotic kits

- Interactive WhiteBoards
- Cameras
- Microphones
- Beebots
- RM Integris
- CCTV
- Walkie talkies
- BBC Micro:bit

Roles and Responsibilities

Head Teacher/Deputy Designated Safeguarding Lead (DDSL)– Nicola Collett-White

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the Designated Safeguarding Lead (DSL) and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance
- 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
- Take overall responsibility for data management and information security (e.g. Integris) ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-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
- 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 cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- 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 that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets ISI requirements
- To approve the Online Safety Policy and review the effectiveness of the policy
- To manage Online Safety Incidents in line with this policy and in partnership with the Online Safety Coordinator
- To receive regular reports from the Online Safety Coordinator
- The Head Teacher will be the first point of contact for any staff misuse of technology
- Organise and meet with Digital Leaders to ensure pupil involvement in online safety

Designated Safeguarding Lead (DSL)/Online Safety Lead (OSL) - Katie Vivyan

- Takes lead responsibility for safeguarding and child protection
- Ensures "An effective approach to online safety [that] empowers a school to protect and educate the whole school in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate." (KCSIE 2021)
- Liaise with the local authority and work with other agencies in line with 'Working together to safeguard children'
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the Head Teacher, DPO and governors to ensure a GDPR-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 safety

- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies, Staff Code of Conduct) and other related documents with the help of the Computing Coordinator and to submit for review to the governors/Head Teacher
- Receive regular updates in online safety issues and legislation, be aware of local and school trends, and make use of outside organisations and agencies (e.g. CEOP/LgfL/CLC)
- Ensure that online safety education is embedded across the curriculum (by using UKCCIS framework 'Education for a Connected World') and beyond, in wider school, including combatting risk of radicalisation e.g. in planning/assemblies
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with SLT and the designated Online Safety Governor/Online Safety Group to discuss current issues (anonymised), review incident logs and filtering/change control logs, discussing effectiveness of filtering and monitoring
- 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 dealt with in the same way as any other safeguarding incidents, and also logged in the Online Safety Incident book (see Appendix 6 for more details)
- Oversee and discuss 'appropriate filtering and monitoring' with governors and ensure staff are aware
- Ensure the 2018 DfE guidance on sexual violence and harassment in a digital context is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff:
    - all staff must read KCSIE Part 1 and all those working with children Annex A
    - all staff must read Annex C (online safety)
    - cascade knowledge of risks and opportunities throughout the organisation
- The OSL will be the first point of contact for any pupil misuse of technology, and if this misuse is a Safeguarding concern will follow normal Safeguarding reporting procedures

Governing Body, led by the Online Safety/Safeguarding Link Governor – Andrea McCallister

- 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 (UKCCIS)
- Ensure an appropriate senior member of staff from the school is appointed to the role of DSL with lead responsibility for safeguarding and child protection, including online safety with the appropriate status and authority and time, funding, training, resources and support
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the DSL/OSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DPO, DSL and Head Teacher to ensure a GDPR-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 staff have read Part 1 of KSCIE; SLT and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in your school
- Ensure that all staff undergo safeguarding and child protection training, including online safety, at induction and that training is regularly updated in line with advice from the SSCP (Southwark Safeguarding Children Partnership)
- Ensure appropriate filters and appropriate monitoring systems are in place, making sure that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum and consider a whole school approach to online safety with a clear policy on the use of mobile technology

All Staff

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job to be vigilant in this area

- Have responsibility to ensure this policy is implemented in conjunction with the school's main safeguarding policy; and to notify the DSL where they see practice that does not reflect policy
- Have responsibility to sign and keep to the terms of their acceptable use policy
- To know the DSL and OSL is Katie Vivyan
- Read Part 1, Annex A and Annex C of KSCIE *
- Embed online safety in teaching, not just when using computers but at other opportune moments and at unexpected moments e.g. during PSHE, literacy (fake news) *
- To supervise and guide pupils carefully when engaged in learning activities (including extra curricular clubs) involving online technology and offline technology, supporting them with search skills, critical thinking, age appropriate materials, signposting, and copyright laws *
- Deal with online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures
- Notify the DSL/OSL of new trends and issues before they become a problem
- Whenever overseeing the use of any technologies in school or setting as homework tasks, encourage sensible use, monitor what pupils are doing and consider potential dangers/the age appropriate websites (ask your DSL what appropriate filtering and monitoring policies are in place) *
- Encourage pupils to follow their acceptable use policy, remind them about it and enforce school sanctions *
- Take a zero-tolerance approach to cyberbullying and low-level sexual harassment in a digital context (your DSL will disseminate relevant information from the new DfE document on this)
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safety issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and the professional reputation of the staff

PSHE Coordinator – Nicola Collett-White

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE curriculum, "complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds."
- Work closely with the DSL/OSL/Computing Coordinator and all other staff, ensuring embedding and a shared understanding of issues

Computing Coordinator – Stephen Lowries

- As listed in the 'all staff' section, plus:
- Oversees the delivery of the online safety element of the Computing curriculum
- Runs Digital Leader meetings where pupils act as online safety ambassadors, running assemblies and regularly being updated about changing practice within the school in an appropriate way
- Acts as a receiver of pupil feedback regarding online safety issues and then feeds this back to the DSL/OSL
- Regularly consults with the DSL/OSL and shares up to date practices and trends
- Refers to the document 'Teaching Online Safety in Schools' when planning the curriculum
- Consults with the DSL/OSL/Head Teacher on updates to this policy
- Works closely with all other staff, ensuring curriculum embedding and a shared understanding of issues
- Often will be involved in leading CPD for other members of staff regarding online safety
- Regularly meets with technician and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use policies
- Oversee any pupil feedback on online safety issues (e.g. liaise with Computing Coordinator after Digital leader meetings)

Technician – Krzysztof Jurek with London Connected Learning Centre (CLC)

- As listed in the 'all staff' section, discounting all * statements:
- 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 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 (DPO) – Amy Roseveare

- NB – this document is not for general data-protection guidance; see Data Protection Policy for more details
- Be aware of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education 2020' (KCSIE) and 'Data protection: a toolkit for schools' (April 2018):
    - GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place […] Remember, the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding
- The same document states that the retention schedule for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'
- Work with the DSL, Head Teacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Parents

- To read, understand and promote the school's Pupil Acceptable Use Policies with their child/children
- To consult with the school if they have any concerns about their children's use of technology
- To, where possible, get involved in online safety training offered (e.g. school portal/leaflets)
- To support the school in promoting online safety, regarding model good practice on digital devices

Pupils

- Read, understand, sign and adhere to the Pupil Acceptable Use Policies annually / upon entry to the school
- To understand the importance of reporting abuse, misuse or access to inappropriate materials
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology

- To understand the importance of adopting safe and responsible behaviours and good online practice when using digital technologies outside of school and to realise that the school's Acceptable Use Policies cover their actions outside of school (e.g. social media)
- To understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems
- To contribute to a 'pupil voice' that gathers information of their online experiences
- Digital leaders will run assemblies and help communicate this policy within lessons as online safety ambassadors

Online safety group

- An online Safety group is made up of a senior Digital Leader, the computing coordinator, the OSL/DSL and the Online Safety Governor
- This group will, where possible discuss the practice of this policy and think through any improvements to be made on it/it's practical applications within the school
- Certain members of the group will have opportunities to discuss online safety issues and legislation, the potential for child protection concerns, current issues and any previous reports/near misses that we can learn from

External groups, volunteers, visitors & contractors

- On entrance to the school, read and agree to the 'Guidance for Parents, Visitors & Contractors' (Appendix) sheet which acts as a safeguarding summary, including key safeguarding information and brief instructions on acceptable use of personal digital devices and other technology within the school environment in accessible language, appropriate to these groups
- Report any concerns, no matter how small, to the DSL/OSL named in the summary given to them
- Support the school in promoting online safety and data protection
- Model safe, responsible and positive behaviours in their own use of technology

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:

With parents and pupils

This policy as well as the Pupil Acceptable Use Policies will be posted on the school website and parents are regularly encouraged to read them. On entry to the school community the Pupil Acceptable Use Policies will be signed by all pupils, and will also be resigned annually. Digital leaders will communicate aspects of this policy in assemblies and in class. Parents read a summarised acceptable use statement in bullet point form before entering the school. The Acceptable Use Agreement will be displayed in school in various appropriate places.

With staff and governors

This policy will be read as part of any new member of staff's/governor's induction process, and the Staff & Governors Acceptable Use Policies must be signed. All staff/governors will be asked to reread this policy annually or where updates have been made as well as re-signing the Staff & Governors Acceptable Use Policies annually or where updates have been made. Online safety training for all staff will be regularly given. The OSL/DSL, in conversation with the Computing Coordinator, will seek out opportunities for continuous professional development regarding online safety and encourage the sharing of good practice throughout the school. The policy as well as the Staff & Governors Acceptable Use Policies is available internally on the school network and paper copies are available in the staffroom.

With volunteers/contractors

This policy will be summarised in bullet point form using accessible language appropriate to these groups 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 Southwest 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 on online safety issues and the school's online safety education program
- Provides, as part of the induction process, all new staff, 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

3. Handling Online Safety Incidents and Concerns

Incident management

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSE and Citizenship). General concerns will be handled in the same way as any other safeguarding concern, with details also being added to the Online Safety Incident Book; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the DSL/OSL to contribute to the overall picture or highlight what might not yet be a problem. Non-teaching staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

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

- Safeguarding Policy (includes the procedure for dealing with peer on peer, sexual harassment, prevent)
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside and outside school, and that those from outside school will continue to impact pupils when they come into 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 dealt with in accordance to Appendix 6 and where necessary and urgent, reported to the OSL/DSL on the same day. Any concern/allegation about serious staff misuse is always referred directly to the Head Teacher, unless the serious concern is about the Head Teacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority 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, NCA CEOP, Prevent Officer, Police, IWF). 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 disturbing or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

Actions where there are concerns about a child

As outlined previously, online safety concerns are no different to any other safeguarding concern, therefore the Safeguarding policy with it's flowcharts and appendices should be followed (p.17 of KCSIE 2021), and Appendix 6 of this policy also acts as a guide in terms of sanctions.

Sexting

We refer to the UK Council for Child Internet Safety (UKCCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview for all staff to read, in recognition of the fact that it is mostly someone other than the DSL/OSL 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.

The school DSL will in turn use the full 50-page guidance document including case studies, typologies and a flow chart, as shown in the Appendices, to decide next steps and whether other agencies need to be involved.

It is important that everyone understands that whilst sexting is illegal, pupils can come and talk to members of staff if they have made a mistake or had a problem in this area. There is more information about this in our Safeguarding Policy.

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing) is now a criminal offence, as highlighted in Keeping Children Safe in Education, and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying should be treated like any other form of bullying, and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying. We recognise that bullying can often involve both a mixture of offline and online contexts (see our Anti Bullying Policy for more details).

Sexual violence and harassment in an online context

Part 5 of KCSIE 2021 is particularly helpful in regards to handling sexual violence and harassment cases. Any incident of sexual harassment or violence (online or offline, and digitally) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. We take all forms of sexual violence and harassment seriously, any incidents considered 'low level', whether appearing through online or offline means using digital devices, are still treated seriously and not allowed to perpetuate.

Misuse of technology (devices, systems, networks and 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 Policies as well as in this document. Where pupils contravene these rules, the school behaviour policy will be applied, as well as clear levels of sanctions as found in Appendix 6; where staff contravene these rules, action will be taken as outlined in the Appendix 6 and the Staff Disciplinary Policy and Procedures.

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.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the LCS community, which are also governed by school Acceptable Use Policies. Breaches will be dealt with in line with the school behaviour policy as well as the steps provided in the Appendices (for pupils). Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media posts by a member of the school community, LCS will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Further help and support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with your Safeguarding Policy. The DSL will handle referrals to local authority Multi-Agency Safeguarding Hubs (MASH) and normally the Head Teacher will handle referrals to the LA Designated Officer (LADO). The local authority, academy trust or third-party support organisations you work with may also have advisors to offer general support.

Beyond this, **reporting.lgfl.net** has a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Whistleblowing Helpline, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people.

4. Data Protection and Security

There are references to the relationship between data protection and safeguarding in KCSIE 2021 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, The Key.

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, 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 into 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.
- The DPO approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought.
- 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).

5. Appropriate Filtering and Monitoring

In line with the KCSIE guidelines, LCS has appropriate monitoring and filtering systems in place so that children cannot access harmful or inappropriate material but at the same time we are aware that "over blocking" and work to make sure that unreasonable restrictions are not put in place.
This school:

- Informs all users that Internet/email use is monitored
- Has educational filtered secure broadband connectivity provided by EXA networks; a group approved according to the UK Safer Internet Centre standards
- This means we have a dedicated and secure connection that is protected with firewalls and layers of security, including a web filtering system called Surf Protect Quantum; which blocks sites that fall into categories (e.g. adult content, race hate, and gaming). We can also retrospectively monitor every user's online behaviour/search history. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

At LCS, we have decided that a combination of option 1 and 2 is appropriate in view of our Prevent Risk Assessment.

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.

6. Electronic Communications

This section only covers electronic communications.

Email:

- Pupils in KS1 and 2 have access to 2Email accounts from 2simple software Purple Mash
- Pupils in KS2 also have access to Gmail, managed through Google Admin
- 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 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 Faye Martin (School Administrator). School Website Design Agency 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: uploading to school approved cloud platforms, displays around the school, 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.

Helen Catt 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.

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. Makewaves/Purplemash/Google Suite), 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 which is separate from the one the children access.

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).

- 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 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: February 2022
Review date: February 2023

A1 – KS1 Acceptable Use Policy (with summary poster)

AUP review date: February 2022
Date of next review: February 2023
Who has reviewed this: Katie Vivyan (DSL/OSL)

We take e-safety really seriously at LCS. We want all children to be 'safe cyber citizens'. Above you can see the e-safety rap that we learn. It summarises much of the teaching children receive regarding staying safe online. It also acts as a shortened version of the school contracts that both parents and pupils sign at the start of each year.

E-SAFETY AT LCS
KS1
ONLINE
ACCEPTABLE USE AGREEMENT

ZIP IT
I will not give away any personal information.
I will log out of any account after each session.
I know people online aren't always who they say they are.
I don't change clothes in front of a camera.
I know what I share could stay online forever.
I don't do dares just because someone says.

BLOCK IT
I will only click on icons, sites, games and apps I'm allowed to.
I will only use the Internet with a teacher.
I will only use devices I'm allowed to.

FLAG IT
If I see something I think is unsafe or upsets, worries, scares or confuses me I will always tell an adult.
If I get a funny feeling in my tummy, I will tell an adult.
I ask for help if I'm not sure.

WELL KIND
I will look after the school's computing equipment and treat it carefully as I have been instructed.
I am kind and polite to everyone.

STUDENT NAME .....

STUDENT SIGNATURE .....

DATE .....

DigiSafe

A2 – KS2 Acceptable Use Policy

AUP review date: February 2022
Date of next review: February 2023
Who has reviewed this: Katie Vivyan (DSL/OSL)

E-SAFETY AT LCS
KS2
ONLINE
ACCEPTABLE USE AGREEMENT

This agreement will help keep me safe and help me to be fair to others

- **I am an online digital learner** – I use the school's internet and devices for school work, homework and other activities to learn and have fun. I only use sites, games, apps and devices that my trusted adults say I can. I know my internet and device use is monitored.
- **I am a secure online learner** – I keep my passwords to myself, reset them if anyone finds them out and log out after sessions.
- **I am careful when I click** – I think before I click and don't click on links I don't expect to see and pop-ups. I only download or install things when I know it is safe or has been agreed by trusted adults.
- **I know new friends may not always be who they say** – Unless I have met them face to face, I can't be sure who they are. If I want to meet them I will ask a trusted adult, and never go alone without telling an adult.
- **I am private online** – I only give out private information if a trusted adult says it's okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends. If I turn on location I remember to turn it off again.
- **I keep my body to myself online** – I never change what I wear in front of a camera and remember that my body is mine and mine only, and I don't send any photos without checking with a trusted adult.
- **I say no online if I need to** – If I get asked something that makes me worried or upset or just confused, I say no, stop chatting and tell a trusted adult. I don't have to do something, even if a friend dares me.
- **I am a rule-follower online** – I know that some websites, games and apps have age restrictions and I respect this; I only visit sites, games and apps that my trusted adults have agreed to.
- **I am considerate online** – I do not post, make or share unkind, hurtful or rude messages/ comments and tell my trusted adults if I see these and block bullies.
- **I am part of a community** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
- **I am a friend online** – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed or is worried or upset by things they read, watch or hear. I won't share anything personal about my friend online and I won't share anything I think they might be embarrassed about online.
- **I don't do public live streams on my own** – and I only go on a video chat if my trusted adult knows I am doing it and who with.

(CONTINUES OVERLEAF)

DigiSafe

E-SAFETY AT LCS

KS2

ONLINE

ACCEPTABLE USE AGREEMENT (CONTINUED)

- **I communicate and collaborate online** with people I know and have met in real life or that a trusted adult knows about.
- **I am a creative digital learner online** – I don't just spend time online to look at things from other people; I get creative to learn and make things!

- **I am a researcher online** – I use safer search tools approved by my trusted adults. I understand that not everything online can be believed, but I know how to check things and know to 'double check' information I find.
- **I ask for help if I am scared or worried** – I will talk to a trusted adult if anything upsets or worries me on an app, site or game - it often helps. If I get a funny feeling, I talk about it.

- **I know it's not my fault if I see or someone sends me something bad** – I don't need to worry about getting into trouble, but I mustn't share it. Instead, I will tell someone. If I made a mistake, I don't try and hide it but tell.

- **I tell my parents / carers what I do online** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I am doing.
- **I respect others' work online** – I only edit or delete my own digital work and only use other people's with their permission or where it is copyright free / has a Creative Commons licence.

- **I protect my online reputation** – I know anything I share might stay online forever.

- **I take screen breaks** – I know that lots of screen time can be bad so I get outside and enjoy the world lots too.

STUDENT NAME .....

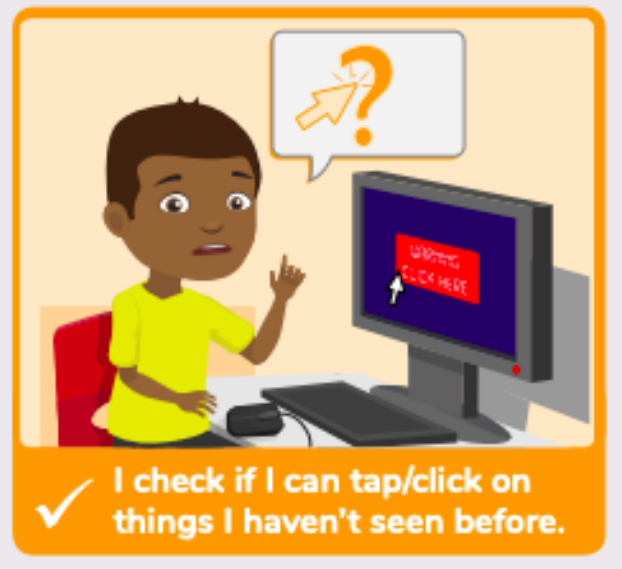
STUDENT SIGNATURE .....

DATE .....

DigiSafe

A3 - ER/R Acceptable Use Policy

AUP review date: February 2022
Date of next review: February 2023
Who has reviewed this: Katie Vivyan (DSL/OSL)



A4 – Staff and Governor Acceptable Use Policy

AUP review date: February 2022
Date of next review: February 2023
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 – I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture, but only if I tell somebody. I have read the sections on handling incidents and concerns about a child in general, sexting, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.
15. 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
k.vivyan@londonchristianschool.com
020 3130 6430

Deputy Designated Safeguarding Lead
Miss Nicola Collett-White
Head Teacher
n.collett-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/DDSL 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

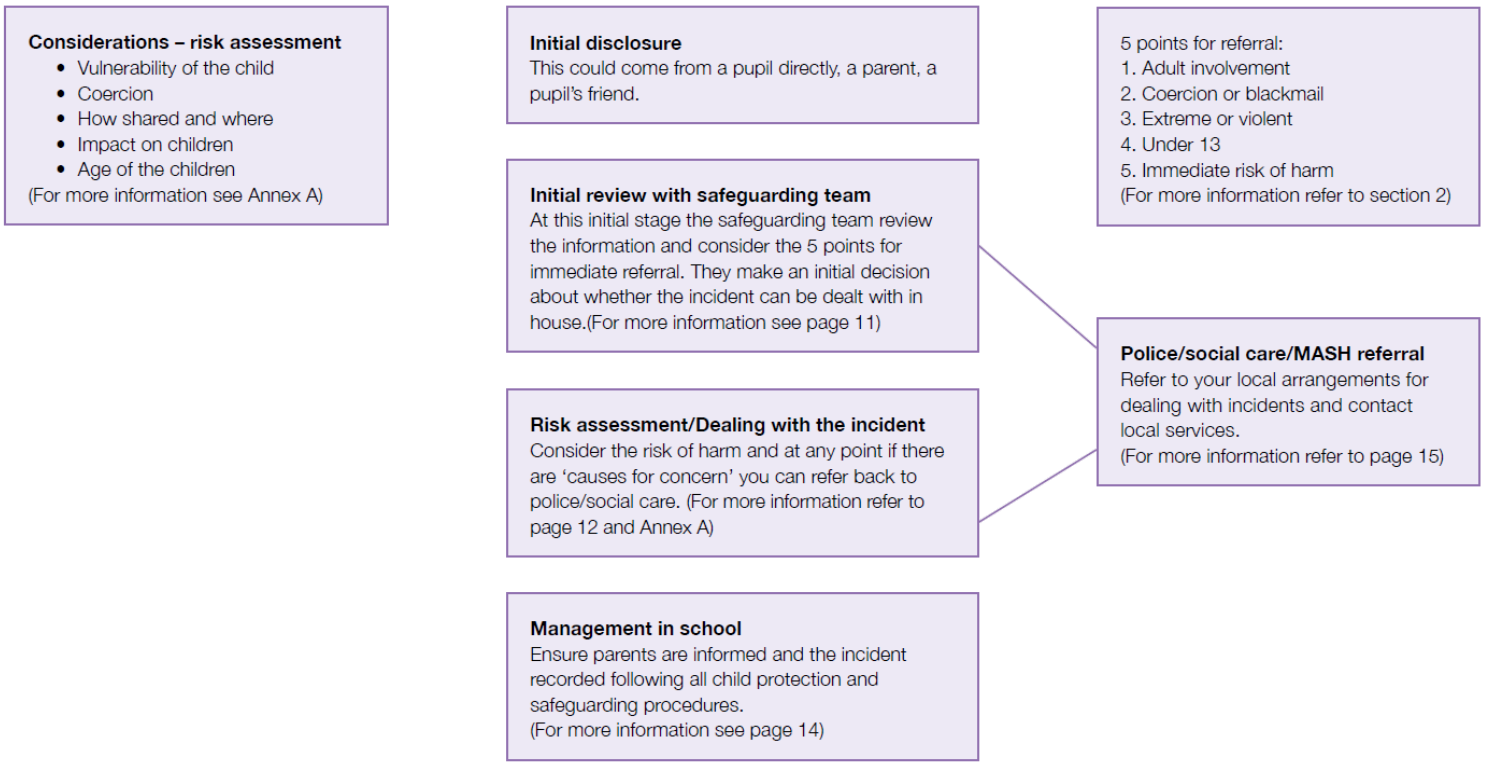
- We use CCTV monitoring as part of maintaining physical security on our premises and is clearly signposted
- LCS is committed to protecting personal data by collecting, processing and sharing data in accordance with current Data Protection Law. You can find our Privacy Notice on our website or ask for 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.**

A6: Handling Sexting and Nude Selfie incidents

The below Flowchart is for information only and must be viewed in the context of the full document; UKCCIS guidance on sexting (also referred to as 'youth produced sexual imagery') in schools.

Annex G

Flowchart for responding to incidents



A7: 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.

PUPIL

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 itemsonline • 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 staff of it	**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 (Gross Misconduct)	**Possible Sanctions**
• Serious misuse of, or deliberate damage to, any school computer hardware or software • Any deliberate attempt to breach data protection or computer security rules • Deliberately creating, accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent • Accessingwebsites advocating violent extremism • Receipt or transmission of material that infringes the copyright of another person or	**Refer to Head Teacher** **Escalate to:** Head Teacher/governors/suspension or dismissal **Other safeguarding actions:** Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.

infringes the conditions of the Data Protection Act, revised 1988 ● Bringing the school name into disrepute	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	

A8: Template for conversations (verbally on via email) for under age viewing/gameplay

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