St Luke's Online-Safety Policy

Introduction

Key people / dates

St Luke's CE Primary School	Designated Safeguarding Lead (DSL) team	**Rachel Goplen**
	Online-safety lead	**Rachel Goplen**
	Online-safety / safeguarding link governor	**Simon Barnes**
	PSHE/RHE and Sex Education Lead	**Mark Gannaway**
	Network manager / other technical support	**Merlin Computing / Hampshire IT**
	Date this policy was reviewed and by whom	**Autumn 2026**
	Date of next review and by whom	**Autumn 2027**

What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2025 (KCSIE), 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 2019 and other statutory documents. It complements existing subjects including Computing and Health, Relationships and Sex Education; it is designed to sit alongside our school's statutory Child Protection and Safeguarding Policy. https://www.st-lukes.hants.sch.uk/policies/ Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

Who is it for; when is it reviewed?

This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. We have developed this policy in line with DfE Covid Safeguarding Guidance and in light of changing needs, potential closure, remote learning and alternative arrangements at school. Acceptable Use Policies (see https://www.st-lukes.hants.sch.uk/policies/) for different stakeholders are reviewed alongside this overarching policy. Any changes to this policy will be immediately disseminated to all stakeholders.

St Luke's Online-Safety Policy

Who is in charge of online safety?

We have a named online-safety lead at our school (see p:1); this person is also the designated safeguarding lead (DSL) and in line with KCSIE, "the designated safeguarding lead will take **lead** responsibility for safeguarding and child protection (including online safety)."

What are the main online safety risks today?

Online-safety risks are traditionally categorised as one of the 3 Cs: Content, Contact or Conduct (identified by Professor Tanya Byron's 2008 report "Safer children in a digital world"). These three areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three.

Many of these new risks are mentioned in KCSIE, e.g. extra-familial harms where children are at risk of abuse or exploitation to multiple harms in situations outside their families including sexual exploitation, criminal exploitation, serious youth violence, upskirting and sticky design.

In past and potential future **remote learning and lockdowns**, there is a greater risk for grooming and exploitation (CSE, CCE and radicalisation) as children spend more time at home and on devices.

How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document, accessible to all stakeholders, communicated in the following ways:

- Posted on the school website at https://www.st-lukes.hants.sch.uk/policies/
- Available on the internal staff network/drive in Curriculum / Policies Folder
- Part of the school induction pack for all new staff
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, governors, pupils and parents/carers https://www.st-lukes.hants.sch.uk/policies/
- Shared with the whole school community along with AUPs, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review
- AUPs for pupils shared with pupils in each class
- Reviews of this online-safety policy to include input from staff, pupils and other stakeholders, helping to ensure further engagement

St Luke's Online-Safety Policy

Contents

Introduction 1
Key people / dates 1
What is this policy? 1
Who is it for; when is it reviewed? 1
Who is in charge of online safety? 2
What are the main online safety risks today? 2
How will this policy be communicated? 2
Contents 3
Overview 5
Aims 5
Further Help and Support 5
Scope 5
Roles and responsibilities 6
Headteacher – RACHEL GOPLEN 6
Designated Safeguarding Lead / Online Safety Lead – RACHEL GOPLEN 7
Governing Body, led by Online Safety / Safeguarding Link Governor – SIMON BARNES 8
All staff 9
RHE and Sex Education Lead – MARK GANNAWAY 10
Computing Lead – LUCY LAMB 11
Subject leaders 11
Network Manager/technician – MERLIN COMPUTING / HAMPSHIRE IT 12
Data Protection Officer (DPO) – BUSINESS MANAGER 12
Volunteers (including any tutors) 13
Pupils 13
Parents/carers 14
External groups including parent associations – FOSLSS 14
Education and curriculum 15
Handling online-safety concerns and incidents 15
Actions where there are concerns about a child 16
Sexting 18
Upskirting 19

Bullying 19
Sexual violence and harassment 19
Misuse of school technology (devices, systems, networks or platforms) 19
Social media incidents 20
Data protection and data security 20
Appropriate filtering and monitoring 21
Email 21
School website 22
Cloud platforms 22
Digital images and video 23
Social media 24
St Luke's School Social Media presence 24
Staff, pupils' and parents' Social Media presence 24
Device usage 26
Personal devices including wearable technology and bring your own device (BYOD) 26
Network / internet access on school devices 27
Other Key Documents 27

St Luke's Online-Safety Policy

Overview

Aims

This policy aims to:

- Set out expectations for all **St Luke's School** community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- 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
- 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
    - 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 and Aggressive Behaviour Policy see https://www.st-lukes.hants.sch.uk/policies/)

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 our Child Protection and Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and normally the headteacher 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 that are available for parents, along with anonymous support for children and young people.

Scope

This policy applies to all members of the **St Luke's CE Primary School** community (including teaching and support staff, supply teachers and any tutors engaged under the DfE National Tutoring Programme,

governors, volunteers, pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Roles and responsibilities

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

Headteacher – RACHEL GOPLEN

Key responsibilities:

- Support safeguarding leads and technical staff as they review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards (see coronavirus.lgfl.net/safeguarding) for an addendum to policies and an infographic overview of safeguarding considerations for remote teaching technology
- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead 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 and relevant Local Safeguarding Partnerships
- Liaise with the designated safeguarding lead 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 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 statutory requirements

Designated Safeguarding Lead / Online Safety Lead – RACHEL GOPLEN

Key responsibilities (remember the DSL can delegate certain online safety duties, e.g. to the online-safety coordinator, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education):

- "The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection [including online safety] … this **lead** responsibility should not be delegated."
- Review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards (see coronavirus.lgfl.net/safeguarding for an addendum to policies and an infographic overview of safeguarding considerations for remote teaching technology
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective approach to online safety that empowers the 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."
- "Liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and SENCOs, or the named person with oversight for SEN in a school and Senior Mental Health Leads) on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies."
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply
- Work with the 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 safeguarding and "undertake Prevent awareness training." – see safetraining.lgfl.net and prevent.lgfl.net
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based
- Receive regular updates in online safety issues and legislation, be aware of local and school trends – see safeblog.lgfl.net for examples

- Ensure that online safety education is embedded across the curriculum in line with the statutory RHE guidance and beyond, in wider school life
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents – materials at parentsafe.lgfl.net
- Communicate regularly with SLT and the designated safeguarding and online safety governor to discuss current issues (anonymised), review incident logs and and discuss how filtering and monitoring work have been functioning/helping
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Oversee and discuss 'appropriate filtering and monitoring' with governors and ensure staff are aware. At St Luke's School, we use Hampshire County Council's HPSN2.1 Smoothwall Web Filtering system to operate and control access in school
- Ensure the 2018 DfE guidance on sexual violence and harassment 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, including supply teachers:
    - all staff must read KCSIE Part 1 and all those working with children Annex A
    - it would also be advisable for all staff to be aware of Annex C (online safety)
    - cascade knowledge of risks and opportunities throughout the organisation
    - cpd.lgfl.net has helpful CPD materials including PowerPoints, videos and more
- Pay particular attention to **online tutors**

Governing Body, led by Online Safety / Safeguarding Link Governor – SIMON BARNES

Key responsibilities (quotes are taken from Keeping Children Safe in Education)

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board
- Ask about how the school has reviewed protections for **pupils in the home** (including when any online tutors are used) and **remote-learning** procedures, rules and safeguards (see coronavirus.lgfl.net/safeguarding) for an addendum to policies and an infographic overview of safeguarding considerations for remote teaching technology
- "Ensure an appropriate **senior member** of staff, from the school **leadership team**, 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 online-safety co-ordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings

- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DPO, DSL and headteacher 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 school staff have read Part 1 of KCSIE; 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
- "Ensure appropriate filters and appropriate monitoring systems are in place but be careful 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"

All staff

Key responsibilities:

In particular attention to safeguarding provisions for **home-learning** and **remote-teaching technologies** (see coronavirus.lgfl.net/safeguarding) for an infographic overview of safeguarding considerations for remote teaching technology. There are further details in the staff AUP.

- Recognise that **RHE** is a whole-school subject requiring the support of all staff; online safety is a core part of this
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know that the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) is Rachel Goplen.
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy and code of conduct
- Notify the DSL/OSL if policy does not reflect practice in our school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RHE and Sex Education curriculum, 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)

- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place)
- When supporting pupils remotely, be mindful of additional safeguarding considerations – refer to the **20 Safeguarding Principles for Remote Lessons** infographic which applies to all online learning
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR
- Discuss roles and responsibilities when using the system at the outset
- Only deliver live- streamed sessions through Microsoft Teams, GSuite, the school approved platforms during normal school hours
- Start any live sessions ahead of scheduled time to allow prompt start to a session.
- Ensure that no sessions with children present are recorded
- Notify children of any resources required during the session
- Be aware of security best-practice at all times, including password hygiene and phishing strategies
- Prepare and check all online source and resources before using them
- Ensure that a one to one situation at the end of an online session is prevented by ending sessions for all participants
- Encourage pupils to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment (refer to the 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 safeguarding 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 of the professional reputation of all staff. More guidance on this point can be found in this Online Reputation guidance for schools.

RHE and Sex Education Lead – MARK GANNAWAY

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives."
- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within RHE and Sex Education
- Ensure that RHE and any additional Sex Education policy should now be included on the school website
- Work closely with the Computing lead to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

Computing Lead – LUCY LAMB

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the RHE and Sex Education lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Subject leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the new RHE and Sex Education curriculum, and model positive attitudes and approaches to staff and pupils alike

- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in our context
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Ensure subject specific action plans also have an online-safety element

Network Manager/technician – MERLIN COMPUTING / HAMPSHIRE IT

Key responsibilities:

- Support the HT and DSL team as they review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards (see coronavirus.lgfl.net/safeguarding for an addendum to policies and an infographic overview of safeguarding considerations for remote teaching technology)
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead to ensure that school systems and networks reflect school policy
- Ensure the school understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files etc)
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team
- 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

Data Protection Officer (DPO) – BUSINESS MANAGER

Key responsibilities:

- Be aware of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document:
- "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful 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. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to

seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant 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."

- Work with the DSL, headteacher 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

Volunteers (including any tutors)

Key responsibilities:

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

Pupils

Key responsibilities:

- Read, understand and ensure that expectations in the pupil acceptable use policy are followed.
- Treat **home learning during any isolation/quarantine or bubble/school lockdown** in the same way as regular learning in school and behave as if a teacher or parent were watching the screen
- Avoid any private communication or use of personal logins/systems to arrange meetings with school staff or tutors
- If parents have consented, take part in virtual and remote learning organised by the school using Microsoft Teams, GSuite for Education in school and at home, making sure that the room that they are in is a room where other family members are not able to disturb the session
- If at home, make sure any additional games consoles and music in the background are turned off
- Make sure they are dressed appropriately and show respect for everyone in the online classroom
- Not disrupt the learning of others
- Not make recordings / images / take screenshots of the class teacher or any part of the session using any device
- Not initiate any live streaming or contact outside of the scheduled session
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor

- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else
- Understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- 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

Parents/carers

Key responsibilities:

- Read and follow the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their 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, pupils or other parents/carers
- Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns
- Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. Ensure the background is blurred or changed where possible
- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately

External groups including parent associations – FOSLSS

Key responsibilities:

- Follow expectations in the acceptable use policy for volunteers prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their 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, pupils or other parents/carers

St Luke's Online-Safety Policy

Education and curriculum

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

- Relationships and Health Education (RHE) and Sex Education (SE).
- Computing

However, as stated in the role descriptors 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).

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), 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.

At St Luke's School, we recognise that online safety and broader digital resilience must be threaded throughout the curriculum.

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing and RHE.)

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Support 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 and Child Protection Policy

- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- 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 school and outside school (and that those from outside school will continue to impact on pupils when they come into school or during extended periods away from school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

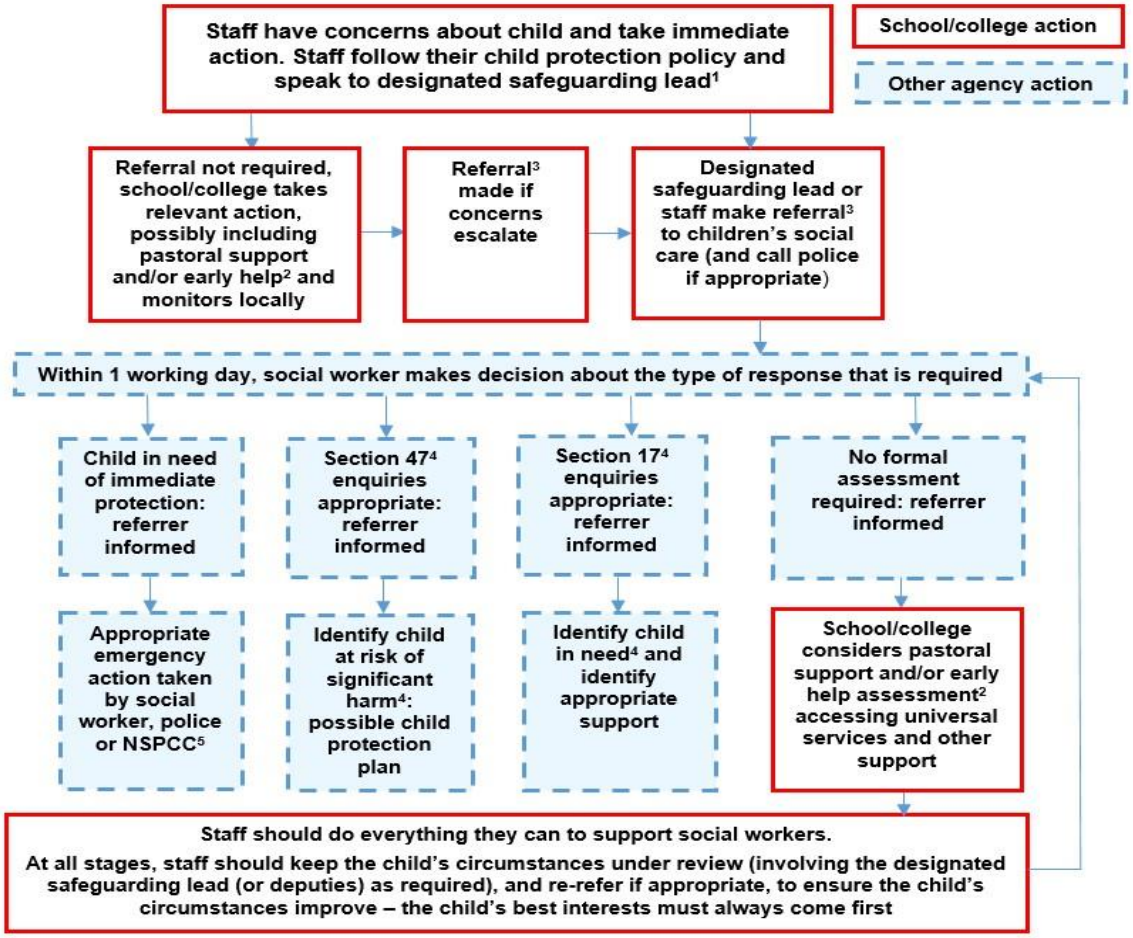
Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, 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

Where there are concerns about a child, the school will take the following actions:

St Luke's Online-Safety Policy



St Luke's Online-Safety Policy

Sexting

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) 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.

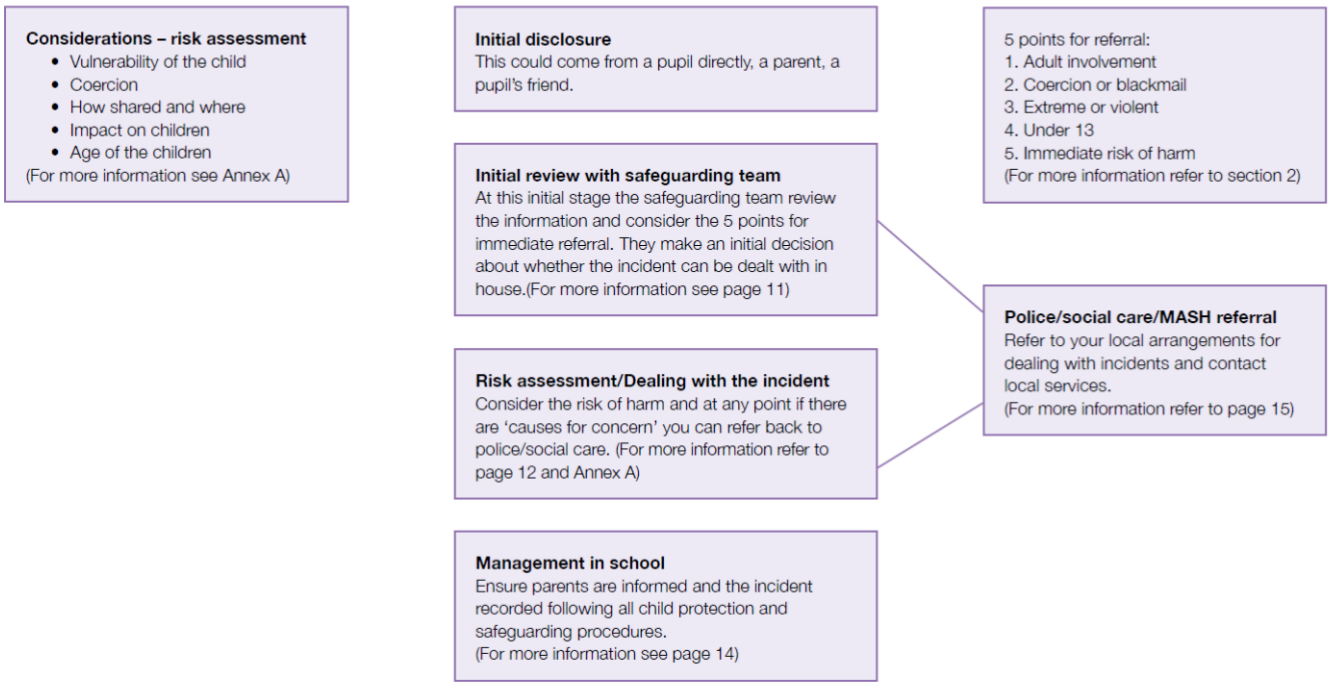
There is a one-page overview called Sexting; how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it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

The school DSL will in turn use the full guidance document, Sexting in Schools and Colleges 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.

Annex G

Flowchart for responding to incidents



The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils 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, including issues arising from banter. The school has an antibullying policy. See Curriculum / Policies.

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

Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education and also a document in its own right. Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

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

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

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

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

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that **the same applies for any home learning** that may take place in future periods of closure/quarantine etc.

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

Social media incidents

Rules and expectations of behaviour for children and adults in relation to social media are outlined in our Acceptable Use Policies and our **St Luke's School Social Media Guide.**

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, St Luke's School 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.

Data protection and data security

GDPR information is in our Data Protection Policy.

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), which the DPO and DSL will seek to apply. This quote from the latter document is useful for all staff – note the red and purple highlights:

"**GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe.** Lawful 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. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) **it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant 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**."

All pupils, staff, governors, volunteers and parents are bound by the school's data protection policy and agreements.

Rigorous controls on the school network, firewalls and filtering all support data protection.

The headteacher, data protection officer 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.

Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place and not be able to access harmful or inappropriate material but at the same time be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

At this school, the internet connection is provided by Hampshire County Council. This means we have a dedicated and secure, school safe connection that is protected with firewalls and multiple layers of security, including a web filtering system called Fortigate which is made specifically to protect children in schools.

There are three types of appropriate monitoring. 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 St Luke's School, we use physical monitoring alongside our webfiltering system to control internet and web access in school. When pupils log into any school system on a personal device, activity may also be monitored here.

Where children are using their own devices at home, parents are asked to supervise and ensure that potential parental controls are in place. Advice for parents can be found at https://www.internetmatters.org/parental-controls/

Email

- Pupils at this school use Office 365 emails or Gmail
- Staff at this school use Office 365 or Gmail for all school emails

This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email used in the chat functionality of Google Classroom, our virtual learning environment, as a Homework submission tool, etc is the only means of electronic communication to be used between staff and pupils (in both directions). Use of a different platform must be approved in advance by the headteacher in advance. 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 Headteacher (if by a staff member).

- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Staff or pupil personal data should never be sent/shared/stored on email. Internally, staff should use the school network, including when working from home when remote access is available via the remote system set up by Coretek or the school's cloud. SIMS and GSuite may also be used.
- Appropriate behaviour is expected at all times, and systems 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 allowed to use the email system for reasonable (not excessive, not during lessons) personal use but 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.

See also the social media section of this policy.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. All staff are able to update various sections of the website. The site is managed / hosted by Primary Site.

The DfE has determined information which must be available on a school website.

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

- School have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. There are many open-access libraries of high-quality public-domain images that can be used (e.g. pixabay.com for marketing materials – beware some adult content on this site).
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

Cloud platforms

It is important to consider data protection before adopting a cloud platform or service – see our DP policy www.st-lukes/policies/ . At St Luke's, we use Microsoft's Office 365, Google for Education's G Suite, Google Drive for file storage.

GSuite for Education, Microsoft Teams, collect, use, and disclose information about users only for the purposes described in the GSuite, Microsoft Teams Privacy notices available here

https://gsuite.google.com/terms/education_privacy.html https://privacy.microsoft.com/en-us/privacystatement / ,

For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush – never share it with anyone!"), expert administration and training can help to keep staff and pupils safe, and to avoid incidents.

The following principles apply:

- 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 when they can demonstrate an understanding of what data may be stored and how it can be seen.
- Pupil images/videos are only made public with parental permission.
- Only school-approved platforms are used by pupils or staff to store pupil work.

Digital images and video

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- For media use
- In printed publications – the newsletter, the prospectus
- In online publications – the school website
- For social media - Twitter
- In videos / or webcams
- For use in online learning platforms – Gsuite for Education, Microsoft Teams
- For use in live stream sessions via GSuite for Education, Microsoft Teams
- For use in online Collective worship and church services with a wider public audience also attending virtually - parents and church members.

Whenever a photo or video is taken/made, a live stream set up, the member of staff organising it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full 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 St Luke's School, no member of staff will ever use their personal phone to capture photos or videos of pupils.

Photos are stored on the school network 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.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include parents or younger children.

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

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), that 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 / or a friend are subject to bullying or abuse.

Social media

St Luke's School Social Media presence

Even though we do not have a Facebook account, 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. The School Office and HT are responsible for managing our Twitter account.

Staff, pupils' and parents' Social Media presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community are expected to follow, 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 have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause

upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school sometimes has to deal with issues arising on social media with pupils under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that online harms regulation is likely to require more stringent age verification measures over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. 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 (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to refer to the Top Tips for Parents poster along with relevant items from parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

The school has an official Twitter account managed by the school office team and will respond to general enquiries about the school, but asks parents/carers not to use these channels to communicate about their children.

Email is the official electronic communication channel between parents and the school, and between staff and pupils.

Pupils are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers or otherwise communicate via social media.

Pupils are discouraged from 'following' staff, governor or volunteer public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public pupil accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher, and should be declared upon entry of the pupil or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

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, or local authority, bringing the school into disrepute.

St Luke's Online-Safety Policy

The serious consequences of inappropriate behaviour on social media are underlined by the fact that of the 131 Prohibition Orders issued to staff in 2017, 73 involved social media/technology (and 27 of the 66 orders by August 2018).

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 (see page 23) and permission is sought before uploading photographs, videos or any other information about other people.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community are expected to follow are also relevant to social media activity, as is the school's Data Protection Policy.

Device usage

We will remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. 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.

Personal devices including wearable technology and bring your own device (BYOD)

- **Pupils** are not allowed to bring mobile phones in to school. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the Digital images and video section on page 23 and Data protection and data security section on page 20. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.
- **Volunteers, contractors or governors** should leave their phones in their pockets and turned off. 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 headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents** should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital images and video section of this document on page 23. Urgent messages can be passed via the school office.

St Luke's Online-Safety Policy

Network / internet access on school devices

- **Pupils** are not allowed networked file access via personal devices. However, 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.
- **Home devices** for vulnerable pupils / from the DfE scheme may be issued to some pupils. If devices are to be taken home, they will be configured with sufficient parental controls to ensure that children can only access required applications.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the Digital images and video section on page 23 and Data protection and data security section on page19. Child/staff data should never be downloaded onto a private phone.
- **Volunteers, contractors, governors** can access the guest wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.
- **Parents** have no access to the school network or wireless internet on personal devices. All internet traffic is monitored.

Other Key Documents

This policy has been written in line with other key documents as outlined below.

1. St Luke's School Social Media Guide
2. Child Protection Policy
3. Safeguarding Policy
4. Behaviour Policy / Anti-Bullying Policy
5. Staff Code of Conduct
6. *Acceptable Use Policies (AUPs) for:
    - *Pupils KS1 / KS2 /
    - *Staff, Volunteers Governors
    - *Parents
7. *Letter to parents about consent to use GSuite, Microsoft Teams and Smart Newro streaming school events
8. *Working together to safeguard children (DfE)
9. *Sexual violence and sexual harassment between children in schools and colleges (DfE advice)
10. *Sexting guidance from UKCIS
    - *Overview for all staff
    - *Full guidance for school DSLs
11. *Prevent Duty Guidance for Schools (DfE and Home Office documents)
12. *Preventing and tackling bullying (DfE)
13. Cyber bullying: advice for headteachers and school staff (DfE) – find this at bullying.lgfl.net