

Annual School Online Safety Audit & Risk Assessment

According to Keeping Children Safe in Education 2026, “Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face.” This document is designed to help schools complete such an assessment.

It is vital that an online safety audit is neither treated as a tick box exercise, nor viewed as a static report: it should be a living document that reflects the fluid realities of technological change, evolving harms and user behaviours.

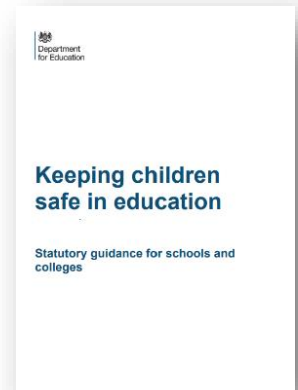
An online safety audit should be carried out by or with the safeguarding team, in recognition that “the designated safeguarding lead should take lead responsibility for safeguarding and child protection (**including online safety**)” (Keeping Children Safe in Education 2026, emphasis added).

Results, conclusions and actions are incorporated into the school’s overall safeguarding audit and considered as part of a holistic, contextual safeguarding approach – not treated separately to offline issues.

This audit has been broken down into two broad sections:

- Curriculum, General Approach & Communication
- Safe School Systems (technology for safeguarding and safeguarding for technology)

Evidence, links, details and when it was checked, plus risks and actions/mitigations (by way of documenting risk assessment) are used in the final check box.



Annual School Online Safety Audit & Risk Assessment

Birkenhead and Mr Somers at Roselyn House School. The audit is reviewed annually in September.

Annual School Online Safety Audit & Risk Assessment

CURRICULUM, GENERAL APPROACH & COMMUNICATION

An effective whole-school approach requires consistency, a common understanding and clear communication. Unless everyone follows a common approach, you communicate clearly with all stakeholders, and staff know what others are doing, there will be gaps. The same will apply if policies do not reflect practice. And always remember, online safety = online safeguarding = safeguarding.

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	- Evidence / details and dates - Any actions / by whom? - Add colour highlights for items to add to risk register <i>NB – we pre-filled examples / links – delete as appropriate</i>
APPROACH				
Approach: whole-school & safeguarding-driven – how does the school demonstrate a whole-school approach to online safety, as particularly advocated in Keeping Children Safe in Education (KCSIE), Teaching Online Safety in School (TOSIS) and subject guidance including Relationships and Sex Education and Health Education (RSHE) and Computing? – is online safety fully accepted as part of safeguarding and therefore not treated as a separate matter, in the eyes of staff, students or parents, and equally in the curriculum and communications, or reflected in incident management and staff roles and responsibilities? – are all staff aware that any discussion of online safety, whether planned or ad hoc, may lead to a disclosure and must be dealt with in line with school safeguarding procedures? – is online safety included on safeguarding reports? – does online safety have obvious involvement of the leadership team and governors? – how does the school ensure that non-specialist staff use consistent approaches and messaging? – does the school take a non-victim-blaming approach (avoiding statements such as “well you shouldn’t be on social media				There is a whole school approach to Online Safety through the PSHE curriculum and the broader curriculum including RSHE. This is visible in the PSHE and RSHE Policy. It is built into schemes of work and is evident in the Collins schemes. Online Safety is accepted as part of Safeguarding and is communicated to staff through policy and training, students through curriculum and Parents/ Carers through updated policy and further information sent out throughout the school year. Staff are fully understanding of disclosure and procedures of recording through CPoms and approaching DSL. They are understanding of contacting the IT Coordinator if they feel there are issues around filtering of the school systems. This is backed up with training through twilight. Online safety is discussed in vulnerable student meetings with DSL’s across whole school. All staff have access to CPoms, if they are agency they are informed to speak to a DSL who will record on their behalf. This is done at induction. Roselyn House School take a non-victim blaming approach

Annual School Online Safety Audit & Risk Assessment

anyway" in response to an incident or disclosure)?			which is notified to staff through training. It may be helpful to reference https://www.gov.uk/government/publications/teaching-online-safety-in-schools
Approach: flexible, current curriculum – how does the school combine an informed, proactive, planned approach with a flexible, reactive approach to ensure it meets changing pupil needs (e.g. as technology changes, trends develop and incidents occur, are they fed into curriculum design and staff training)? – are staff comfortable with making the most of ad hoc opportunities to discuss and learn as online safety conversations arise? – how does the school review annually that teaching is current and relevant to the setting and pupil needs and experiences? – are all the harms and issues and ‘underpinning behaviours’ mentioned in TOSIS and the RSHE guidance addressed throughout the year? – is particular consideration made for vulnerable students, e.g. those with SEND and other needs? – how does the school avoid overlapping teaching, e.g. covering the same issue in different subjects (e.g. RSHE and Computing)? – do you collate ‘pupil voice’ to ensure messaging addresses pupils’ lived experiences? – do you ensure that positive experiences online are also celebrated (not just harms and negative aspects of life online)?			As this is an ever-changing landscape. The designated safeguarding lead/back-ups and senior leadership team ensure that all relevant changes that may impact the safety of our students in tech, trends and viral online incidents, are communicated with the broader staff group. This is to inform staff of information that we are notified of via various school support networks, government publications or online alerts regarding changes that could potentially harm our students. These concerns/content may have arisen from online publications, tech or other multimedia applications. We also encourage all staff to feedback any changes that they may be aware of, as their insight is valuable due to the wider reach of the online community. Everyone has responsibility to ensure the safety of our students. Staff feel comfortable and will have discussions with the students around safety. This is conducted organically (ad hoc) and can be preplanned depending on the information/situation. Conversations, interventions or concerns are all logged on CPOMS and raised with DSLs and SLT. We hold frequent briefings with all staff. We discuss any potential issues that may arise and use the time to conduct relevant staff training. This is a mixture of in house and outsourced training. We use teacher meetings to discuss curriculum changes and any content that may need covering due to incidents/current trends etc. All actions are carefully considered given the needs of our students. We draw from their own personal experiences and utilise this information to

Annual School Online Safety Audit & Risk Assessment

			sensitively deliver any content (Person specific). You may wish to reference/consult: • https://www.gov.uk/government/publications/teaching-online-safety-in-schools • https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education • https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study
Assessment – is the curriculum informed by and measured against clear outcomes, e.g. those in the UKCIS framework Education for a Connected World (or similar)? – how do you use formative and summative assessment to ensure you are aware of pupil knowledge and skills to inform teaching, and subsequently to measure progress			Through teacher and whole school group meetings, this is discussed throughout the academic year. The curriculum is informed by UKCIS framework through PSHE unit 'Internet safety and harms' and other themes throughout the curriculum. Further education and support are offered during individual sessions. Student understanding is tracked using formative and summative assessment of any learning that has taken place on the subject matter. If students are struggling with aspects of the specific topic within the curriculum, further intervention session take place. We also liaise with outside agencies that may be linked to the student or their families; to enhance the support offering of any concerns we may have around vulnerability etc. Education for a Connected World is available at gov.uk/government/publications/education-for-a-connected-world The Safe Skills online safety quiz tool is free for all UK schools to use and includes teacher stats safeskills.lgfl.net

Annual School Online Safety Audit & Risk Assessment

Parental engagement – how do you proactively engage parents/carers? – are parents aware of the school's broad online-safety approach? – are parents aware of the latest harms and issues as well as encouraged to use safety settings on popular platforms, devices, games, apps and consoles? – are parents reminded of the importance of following age ratings? – do you follow a drip-feed approach to communicating with parents?			Parents sign consent forms before a student starts at RHS. All policies are accessible via the school website Regular Online Safety Bulletins are sent to highlight latest harms and issues. Policy and bulletins refer to safety settings. Parents are reminded of following age ratings through emails, letters and discussions. There is a drip feed and supportive approach to communicating with parents and more intense 1:1 discussions take place where appropriate and may involve outside agencies. Resources from parentsafe.lgfl.net may be helpful here and scare.lgfl.net
External influences, resources and scares – are external resources always first assessed for appropriateness (age appropriate, not overly negative, scary, victim blaming etc)? – are any external purchased schemes of work/curricula carefully adapted as necessary? – what approach does the school take to reacting to online challenges, scares and hoaxes? – how are any external visitors vetted for expertise, appropriateness and safeguarding understanding?			All external resources are assessed to ensure they are appropriate and specific to the needs of our students before they are used or distributed. This is done through consultation with DSL, SLT and the wider teaching staff. All curriculum content is adapted to meet the needs of our students. Roselyn House School adapt practice and inform all staff of any challenges that may arise from online content. This is done through via our whole school communication platform and via face-to-face meetings. Again, this is adapted to ensure that staff can feedback any concerns they may have to DSLs and SLT for us to action and discuss with the whole school staff group. External visitors sign in, read visitors protocol and are made aware of the DSLs. SLT are aware of any visits that take place on our grounds (unless unaccounted) in which a member of staff will always direct to SLT. We cannot ensure that all visitors are vetted prior to attending due to the number of visitors, organisations and single parties that we work with throughout an academic year. When working with people that are consistent throughout the year, we ensure that pre checks are conducted to ensure relevant DBS and other checks are

Annual School Online Safety Audit & Risk Assessment

			completed. It may be helpful to reference • scare.lgfl.net • gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes • UKCIS victim-blaming guidance (<i>soon to be published at time of publication of this document</i>) • gov.uk/government/publications/using-external-visitors-to-support-online-safety-education-guidance-for-educational-settings LGfL provides signposting to a range of themed resources at https://saferesources.lgfl.net
POLICIES & PRACTICE			
Policies – do your policies govern all online behaviour, not just when using school devices or logged into school systems and platforms? – do you have an online-safety policy (whether standalone or section within your safeguarding and child-protection policy?) – do you have (note the following might be integrated into other policies and not standalone but must be very clear if so) ○ AUPs to reflect varied roles and responsibilities, e.g. different key stages, parents, staff, visitors, governors, contractors etc. (NB whilst often called “acceptable <u>use</u> policy”, these should reflect all online behaviour). ○ Social media policy? If not, this may be included in your online safety policy but should be clear.			Several organisations provide customisable templates, including LGfL at https://safepolicies.lgfl.net Online Safety Policy- update completed 17.07.2026 Included in Acceptable Use Policy 09.07.2026. AUP informed. Social Media Policy Updated June 14.07.2026

Annual School Online Safety Audit & Risk Assessment

Content & review, policy v. practice – do you consult others to populate your policy, e.g. review templates (LSCP, fellow schools, The Key, LGfL, etc)? – where you have used content or templates, have you checked it is relevant to your setting, systems and stakeholders and adapted as appropriate? – do you regularly review these policies (not just the annual governor review but with staff and pupils who can give insights into practicability)? – how do you check that policies are both followed and possible to follow (e.g. contradictions with other policies, a ban on mobile photography when there are no school cameras and photos are often required, references to systems which no longer exist)? – are new systems, platforms, processes and user behaviour/needs regularly incorporated into these 'living' documents? – are policies updated to reflect curriculum needs, behaviour and safeguarding risks and incidents <u>in your school</u>?			All Policies consult with key guidance and other schools in order to populate policy. Any templates used are checked to be relevant to Roselyn House School Policies are written/ updated by various members of the school leadership team. All Policies are reviewed annually or when guidance changes, These are done in consultation with staff, students, Parents/ Carers. Policies may be updated any time of the year to check these changes or when necessary after a concern review. Our school is across two sites and regular meetings take place with SLT and staff on a daily/weekly basis. Staff have review meetings when Policy is changed/ updated and INSET trainings are used throughout the year including twilight to address these issues also. All new systems, platforms, processes and user behaviour/ needs are incorporated into these documents. Assessment of data/ CPoms is used to make changes to policy, curriculum needs, behaviour and safeguarding risks in the school. Everyone knows students well and safety and wellbeing is paramount. New 'Use of Artificial Intelligence (AI) Policy' introduced September 2026.
TRAINING			
Training & CPD – do all staff receive online safety training as part of the safeguarding training schedule (at induction and start of year or mid-year for new starters)? – is the centre of expertise in online safety within the DSL team			All staff receive Online Safety, Safeguarding and Cyber Security Training through induction and annually. DSL's receive more in depth, advanced Safeguarding Training to incorporate Online Safety. There are 4 DSL's who complete training every 2 Years. They have also completed training in

Annual School Online Safety Audit & Risk Assessment

with the most in-depth training received by this team? – are regular updates given throughout the year, reflecting trends, harms and incidents in school as well as nationally? – is training appropriate to and customised for different roles and responsibilities, with extra strategic elements for SLT and governors? – does training around 'online safety' tie in with training on other areas which may not be classically associated with online safety, such as all the harms mentioned in KCSIE (e.g. Prevent and many others)? – do technical staff receive sufficient training on key safeguarding elements? – do non-technical staff receive sufficient training on technical aspects?		Filtering and Monitoring. Online safety is referred to in all aspects of training with regard to KCSiE, Prevent, Curriculum, IT. Technical staff receive annual Safeguarding and Online Safety Training along with training in Health and Safety, Cyber Security, GDPR and Filtering and monitoring. There are online courses and tutorials available on SharePoint for technical training along with access to IT Co-ordinator support via telephone and Email. Trainings contain information about Online Safety. Free training is available from LGfL at safetraining.lgfl.net And from most LSCPs (Local Safeguarding children Partnerships) Excellent paid training is available from many organisations such as NSPCC.
---	--	---

[END OF SECTION 1]

Annual School Online Safety Audit & Risk Assessment

SAFE SCHOOL SYSTEMS

Schools have a duty to provide safe school systems – this may take the form of technology for safeguarding (e.g. filtering) or safeguarding for technology (such as behaviours or settings to adopt on a particular device or platform).

It is important to remember that technology changes all the time, whether functionality, risks or appropriate settings, and there is always a balance to be struck between safety precautions and 'over-blocking', which Keeping Children Safe in Education requires schools to avoid (the 2022 version includes reference of 'regular review'). The education element is therefore key, i.e. teaching children and young people what to do when they see or experience something worrying.

Safeguarding teams will wish to engage with their technical colleagues on this section – please ensure to review it together.

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	- Evidence / details and dates - Any actions / by whom? - Add colour highlights for items to add to risk register <i>NB – we pre-filled examples / links – delete as appropriate</i>
FILTERING				
Appropriate filtering – has your provider filed a submission with the UK Safer Internet Centre to explain why your filtering is 'appropriate'? – have DSL, SLT and technical teams all read and understood this submission, including rationale, benefits and limitations and safe search settings, e.g. for web searches and YouTube?				A rationale is in the IT Folder on SharePoint including what is allowed and blocked. Safer Internet Centre submissions - https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/filtering-provider-responses YouTube guidance - https://youtube.lgfl.net
Filtering training – has your technical team attended training on your filtering platform/s to understand exactly how it works, how it is set up and what the options are in order to inform a strategic filtering approach and implement DSL/SLT requirements? – has your safeguarding team also attended training to know the questions they need to ask of their technical colleagues and to understand at a high level what filtering can/should do to inform the approach?				D Somers has had Unifi Cybersecure training and Safeguarding Training. He has read KCSIE 2026. Further training from UK Safer Internet Centre for both Tech and DSLs. Tech training - https://lgfl.bookinglive.com/book/add/p/23 Safeguarding training (20 minute overview) - https://lgfl.bookinglive.com/book/add/p/5

Annual School Online Safety Audit & Risk Assessment

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	- Evidence / details and dates - Any actions / by whom? - Add colour highlights for items to add to risk register <i>NB – we pre-filled examples / links – delete as appropriate</i>
Rationale / team effort – do your technical and safeguarding teams meet to discuss your filtering needs and document your approach regarding what is allowed / not in school and the safeguarding-driven rationale? – is this up to date, reflected accurately (and updated) in policies and practice, including how your approach and settings do not 'over-block', and shared with parents, staff and governors and ready to show to Ofsted?				Regular meetings take place between S.Damerall and D Somers also involving J Birkenhead. The approach is documented in policy, audit and risk assessment. There is improved documentation and reporting as it was previously done by discussion. This is accurate and updated. It is shared with staff, Parents/ Carers and ready to show to Ofsted.
Reporting and regular review – do you receive regular automated reports to inform safeguarding / behaviour interventions and review use of the system to keep users safe and ensure you are not overblocking (also important to ensure access to teaching & learning sites)? – who is responsible for checking these reports have been run and are being reviewed, and that they are functioning correctly? – is the system regularly reviewed to ensure appropriate access, settings and usage, including consideration of impact				D Somers completes weekly checks which inform use of Internet and what may have been attempted. Discussions are had with SLT so as to ensure we are not over blocking. There are access to Teaching and Learning sites. If a new site is requested this will be communicated to D Somers who then will check with J Birkenhead to ensure it is allowed. D Somers conducts the reports and these are checked by J. Birkenhead. The system is reviewed on a weekly basis and adjustments made when required. An annual audit is carried out. e.g. Viewing top blocked sites / categories monthly will highlight trends and changes that need to be investigated or addressed by talking to students. Weekly checks are supported by screenshots of the real time Cybersecure monitoring software and are stored on the school's Sharepoint, Mr Birkenhead checks these monitoring logs and signs them off.
Safe modes / search				D Somers is responsible for checks and blocking and reports

Annual School Online Safety Audit & Risk Assessment

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	- Evidence / details and dates - Any actions / by whom? - Add colour highlights for items to add to risk register <i>NB – we pre-filled examples / links – delete as appropriate</i>
– do you enforce safe search on search engines and block those which do not have a safe search? For YouTube, do you enforce one of the restricted modes as appropriate for your needs?				back to J.Birkenhead. Google/ Bing Search Engine is utilised and Safe search is enabled. You Tube Safe search is enabled at all times. We also ensure only Microsoft Edge browsers are installed on client workstations to help prevent any enabling of VPN browsers via add on tabs YouTube mode checked via https://youtubemode.lgfl.net YouTube settings overview at https://youtube.lgfl.net Check at the top right of the search page if Google safe search is enforced (LGfL schools request this via a DNS change)
BYOD – if you allow ‘bring your own device’, what measures are applied to these devices to ensure the school internet cannot be used inappropriately simply by switching to a BYOD network				The school filtering blocks on BOYD devices the same as school devices. NB there are many different approaches – some schools do not allow BYOD; many do or restrict it to certain groups. Some schools insist upon logging in if using the BYOD network; others where this is not possible might choose to make it much more restrictive
Devices at home – have you applied filtering to school devices when sent home with students? – given that schools cannot protect parent/child devices, do you remind parents about how to set controls on their home internet/phones/devices etc?				Devices which have been provided by LA with Internet dongles have LCC filtering. We are investigating improving filtering on devices borrowed from school but the consent/ acceptable use has sections about filtering and monitoring contained. They are monitored on recall. Web filtering for school devices at home is available from various providers including LGfL – those solutions which also

Annual School Online Safety Audit & Risk Assessment

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	- Evidence / details and dates - Any actions / by whom? - Add colour highlights for items to add to risk register <i>NB – we pre-filled examples / links – delete as appropriate</i>
				have Chrome extensions can also protect children if they access a school profile on a family device. We discourage the use of extensions because they can easily add VPN extensions and it's simple to uninstall any web protection add ons. Parents/ Carers are reminded how to set controls and are supported in doing so. See https://parentsafe.lgfl.net for support with parental control settings and other ways parents can keep their children safe online
Linked to the curriculum and safeguarding landscape – is your filtering set up and updated to reflect the online-safety messages you teach and safeguarding concerns/cases in school? – conversely, is learning from filtering findings used to inform the curriculum?				Filtering is updated regularly to reflect safeguarding concerns and is communicated to SLT via the DSL's and IT Coordinator. If there is a spike in filtering findings this is then addressed by year leads and is managed by J Birkenhead. An example for Q2 in this row – if there is a spike in failed attempts to view pornographic sites, is this covered in class as a priority, regardless of where it may fall in the scheme of work / plan for the year?
MONITORING				
Approach – is your approach to monitoring based on a strategic and safeguarding-driven rationale that has been made in discussion between safeguarding and technical teams? – are all senior leaders, governors and staff aware of this rationale and which of the three possible approaches (or combination) outlined by the Safer Internet Centre that your school follows.				D Somers has regular meetings with DSLs and SLT to approach monitoring within a safeguarding driven rationale. All SLT are aware of this as they are involved. We utilise all 3 possible approaches as outlined by the Safer Internet Monitoring Centre. - Physical monitoring - Internet and Web Access

Annual School Online Safety Audit & Risk Assessment

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	- Evidence / details and dates - Any actions / by whom? - Add colour highlights for items to add to risk register <i>NB – we pre-filled examples / links – delete as appropriate</i>
				3. Active/ Pro- active technology monitoring services. Safer Internet Centre monitoring approaches - https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-monitoring
Appropriate monitoring – if you use a pro/active technical monitoring solution, has the provider filed a submission to the UK Safer Internet Centre? – have DSL, SLT and technical teams all read and understood this submission, including rationale, benefits and limitations.				A rationale is in the IT Folder on SharePoint including what is allowed and blocked. The school fully complies with the UK Safer Internet Centre's 2026 guidance as referenced on their website : Appropriate Filtering and Monitoring: What's New for 2026? - UK Safer Internet Centre Safer Internet Centre appropriate monitoring provider submissions – https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-monitoring
Monitoring training – if using a pro/active solution, has your technical team attended training to understand exactly how it works, how it is set up and what the options are in order to inform a strategic approach and implement DSL/SLT requirements? – has your safeguarding team attended training to know the questions they need to ask of their technical colleagues and to understand at a high level what monitoring can/should do to inform the approach?				Cybersecure (unifi) provided by our external IT providers Claritel Ltd have provided training on the new filtering / monitoring software. Discussions have taken place with DSL/SLT with regards to it's implementation. I
System configuration, customisation and review – do your technical and safeguarding teams meet to discuss your monitoring needs and ensure systems are configured for the				Regular meetings take place between D Somers, S Damerall and J Birkenhead.

Annual School Online Safety Audit & Risk Assessment

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	- Evidence / details and dates - Any actions / by whom? - Add colour highlights for items to add to risk register <i>NB – we pre-filled examples / links – delete as appropriate</i>
devices and systems you used and regularly updated/reviewed where changes are made and new devices added to ensure no devices or systems are missed? – are systems customised for your safeguarding needs – e.g. adding keywords that represent new concerns in your school/area or to follow students at particular risk. – is this approach documented and the system regularly reviewed to ensure appropriate access, settings and usage / do your policies reflect practice in school and are they updated when settings / approach are changed?				Weekly vulnerable student meetings take place in which all DSL's are present. This approach is monitored weekly within the CSC & Vulnerable child document, alongside CPOMS logs. Policies are updated annually and are updated as when required.
Reports – if using a pro/active solution, is the system set up in such a way that you have a manageable number of captures and are not overwhelmed and therefore at risk of missing key safeguarding alerts? – do you also run reports to spot trends over time? – are concerns fed into the safeguarding systems you use to capture manual/offline safeguarding concerns to complete the safeguarding jigsaw and not kept in a separate silo?				There are a manageable number of captures which has been agreed with D Somers. The reports spot trends over time and these are recorded on Cpoms or discussions with SLT.
Other – please also consider the school devices when at-home / curriculum / BYOD questions mentioned in the filtering section above and add any aspects not already covered there.				
HOME / REMOTE LEARNING & DEVICES IN THE HOME				
School devices in the home – if you send school devices home with students, how are they				No school laptops/devices are sent home with students

Annual School Online Safety Audit & Risk Assessment

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	- Evidence / details and dates - Any actions / by whom? - Add colour highlights for items to add to risk register <i>NB – we pre-filled examples / links – delete as appropriate</i>
protected / monitored? – do you have internet filtering/monitoring on them? – are they locked down as 'managed devices' so software cannot be un/installed except by school admins?				
Live lessons (even after covid, most schools will now deliver live lessons on scheduled and unexpected days, e.g. open days, elections, snow days, broken boilers, etc.) – do you have a remote learning policy or clause in another policy that covers behaviour for pupils and staff? What key safeguarding precautions are included?				There is an updated Remote Learning Policy 2026-2027. Staff have received training in Remote Learning. The infographic at https://remotesafe.lgfl.net has 20 safeguarding considerations for lesson livestreaming that are good precautions to have in place. Whether you use that list or not, note your high-level precautions here.
Homework / cloud platforms accessible from home (all other platforms that can be accessed at home, whether for homework or during home learning) – are these covered in policies and AUPs and regularly updated as new platforms/systems are bought? – are all systems audited to ensure that they have an audit trail, central administration not limited to one person, oversight of administrators and settings locked down where features are not required, e.g. to not allow unmonitored communications?				Homework tends to be sent out via paper copy but in some instances, may be a web link etc. Policies are updated when new systems are brought in and staff/ Parents/ Carers and AUPs are updated. All systems are audited and monitored between D Somers, S Damerall and J Birkenhead.
GENERAL – ALL TECHNOLOGY USED IN / BY THE SCHOOL				
Safeguarding & technical collaboration and review – do safeguarding and technical teams review at least annually (or whenever significant changes are made to technology or the way the school works or new technologies are adopted), which platforms, systems and devices are used, how, what their settings				All is reviewed annually or when necessary and the information is stored in a specific folder on the school's SharePoint.

Annual School Online Safety Audit & Risk Assessment

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	- Evidence / details and dates - Any actions / by whom? - Add colour highlights for items to add to risk register <i>NB – we pre-filled examples / links – delete as appropriate</i>
allow and why, plus risks and mitigations?				
Communication functionality – are all platforms that include any chat function (remember that ‘comments’ can be used to chat, especially if they are never monitored) included in your policies, AUPs and risk assessments and locked down in the way your school wants them? – are all staff and pupils aware which platforms they can use to communicate between students or between staff and students and that they must never use accounts/emails/apps that are not approved/linked to the school?				All platforms are included in Policy and locked down in accordance. Through policy and training, staff and students are aware of student email to communicate. student@roselynhouseschool.co.uk office@roselynhouseschool.co.uk , website form. The Electronic Information and Communication policy makes it clear which accounts/emails/apps that are not approved/linked to the school where possible.
Technology in your policies / AUPs – are the latest school system, platforms and devices that CAN be used/accessed at home included in your policies/AUPs etc? – have these been updated/audited recently to ensure they are still accurate? – are the rules there possible to follow (e.g. systems named which no longer exist or “use a school camera” when they don’t exist or work)?				Policy and audits have taken place June/ July 2026 and reoccur yearly.
CYBERSECURITY				
Audit & documentation (given its importance for continuity of access to systems and data for keeping children safe, schools secure and maintaining continuity of teaching & learning, cybersecurity should be audited separately) – does your school have the recommended 3 documents from the NCSC: - o cybersecurity policy				There is a Cyber Security Audit and Risk asset register and a Emergency Response Plan and Security Plan which all refer to Cyber Security. These are bespoke to the school and updated June 2025. These meet Ofsted Inspecting Safeguarding requirements and KCSiE 2026.

Annual School Online Safety Audit & Risk Assessment

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	- Evidence / details and dates - Any actions / by whom? - Add colour highlights for items to add to risk register <i>NB – we pre-filled examples / links – delete as appropriate</i>
○ risk + asset registers ○ incident response plan – are these accurate and regularly updated, read by all and reflected in practice? – would these answer the Ofsted <i>Inspecting Safeguarding</i> document’s requirement for systems to protect against cybersecurity risks”?				Templates for these three documents including notes to explain to a non-technical audience are at https://elevate.lgfl.net
Technical staff – do technical staff have training on cybersecurity and report to senior leaders and governors on issues, mitigations incidents and training needs?				The IT Co-ordinator D Somers has training on Cyber Security and reports to SLT on issues, mitigations and training needs. The NCSC questions for governors document may be helpful here – ncsc.gov.uk/information/school-governor-questions
Training – are <u>non-technical</u> staff given training and regular reminders on cybersecurity best-practice (passwords, phishing, reporting and more)?				Cyber Security has been delivered to all staff and is repeated annually from May 2023. NCSC non-technical training for school staff is available for free, e.g. from LGfL https://booking.lgfl.net/book/add/p/33