Dothill Primary School

Online Safety Audit

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
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 PSHE including Relationships and Health Education 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 anyway" in response to an incident or disclosure)?	🟩			As stated in KCSIE, pupils are safeguarded from potentially harmful and inappropriate online material. Pupils are taught about the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app and is done so via PSHE lessons, computing lessons and assemblies. Teaching about online safety and harm is a whole school approach. An online safety questionnaire was carried out with the whole of KS2 to identify any concerns around online safety and their online behaviour outside of school. As a school, we understand the risks that exist online and have tailored our teaching, assemblies and support to the specific needs of our pupils. Action: Results of recent survey will be analysed to ensure that we are tailoring our teaching / parental support more effectively. Through PSHE lessons, pupils learn about e-safety, which focus specifically on the eight different aspects on online education in accordance to the Education for a Connected World framework: • Self-image and identity • Online relationships • Online reputation • Online bullying • Managing online information • Health, well-being and lifestyle • Privacy and security • Copyright and ownership

	🟩			In computing lessons, pupils are taught to be safe online; recognise acceptable/unacceptable behaviour and identify a range of ways to report concerns about content and contact on the internet or other online technologies. The governors ensure online safety is high priority and know the approach to safeguarding and related policies and procedures. Online safety concerns are recorded in the same manner as any other safeguarding concern. These are recorded on CPOMS for investigation and action. All staff know how to report a safeguarding concern and pass this to a DSL in a timely matter. Safeguarding is the responsibility of everyone in our school. If disclosures are made, staff deal with them in line with school safeguarding procedure and are aware that learning about online safety in school could lead to these. Safeguarding procedures, including Online Safety, are regularly reported to the Governing Body in Committee and Full Governing Body Meetings where a Headteacher Report is provided with relevant updates. Action: CPOMS Categories to be updated to enable filtering of Online Safety Incidents. From this, reports can be generated and reviewed in DSL meetings. Teaching staff have undertaken online safety CPD from the Online Safety Alliance to improve their understanding of online safety and the risks that are posed for our children. Computing CPD is planned within Termly Staff Meetings to ensure that any updates are shared with staff. Safeguarding is an agenda item for every staff meeting so any online safety concerns can be raised, as they arise. Minutes of staff meetings are saved so that all staff can access these. In the event of concerns relating to Online Safety e.g. Social Media, Messaging Apps etc, concerns are passed to a DSL, who investigates what has happened. When relevant, contact is made with parents to raise their awareness and alert them to any age restrictions. The

	🟩			newsletter is also used to communicate online safety advice, as is the school website and the school's social media platform. Children involved in an online safety concern are then educated and reminded about the dangers posed online and what they need to do to keep safe.
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)?		🟨		School plan opportunities to gain pupil voice around their online behaviour and review this as DSLs to identify any trends or concerns. These are then reacted to in a timely manner through assemblies and lessons across school or in a specific year group. Staff training needs are reviewed and addressed through weekly staff meetings or specific CPD, if required. Within lessons, teachers respond to matters that arise in discussions in an age-appropriate way. At the start each academic year, pupils sign the 'Acceptable Use' agreement to help keep them safe. This is on display in class and regularly referred to. The curriculum is reviewed at the end of the summer term and changes are made where necessary. Assembly focus is reviewed regularly to ensure they are responsive to current needs. Throughout the year, teaching covers how to evaluate what they see online, how to recognise techniques used for persuasion, online behaviour, how to identify online risks and how and when to seek support. Understanding and applying the knowledge and behaviours above will provide pupils with a solid foundation to navigate the online world in an effective and safe way. Action: Evaluate the current teaching of online safety. Does the Jigsaw curriculum need to be supplemented with other resources? There are clear progression documents in place for PSHE and Computing. Safeguarding Squad members created a survey to evaluate children's online habits. Pupil surveys have been completed in KS2 and pupil voice around online safety has taken place. The Safeguarding Squad led the assembly on online safety during Safer Internet Day.

		🟧		Action: Safeguarding Squad to collate the information from the pupil survey and will lead assemblies which will focus on any issues raised from the surveys. Pupils have positive online experiences and enjoy their computing lessons. They understand search engines can be used to locate useful information to support their learning.
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		🟧		In school, there are clear progression documents in place to ensure that the taught curriculum has clear outcomes. Pupils record work linked to Online Safety in PSHE in their class floor book. Formative assessment takes place in every lesson through observing, listening, questioning, discussing and reviewing pupils' work.
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 are updated throughout the year about the importance of online safety. They receive this information through the school newsletter and are aware that information can also be found on the school website. Parents have been advised of the age limits of social media applications and online harm and issues to enable them to make informed choices to keep their child safe online. Parents were invited to digital literacy courses, run by T&W. Parents can access the Online Safety Policy on the school website. They are signposted to this via the school newsletter. There is a further online safety page with advice and links.
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	🟩			Any resources used in school to raise online safety awareness are reviewed and checked to ensure they have clear messages that are age-appropriate and not overly negative or scary. NCCE's Teaching Computing is used for Computing Lessons including Online Safety.

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?	🟩			As a school, we ensure that any purchased resources that include elements of online learning, are checked by teaching staff and password protected for both teachers and children. If there are safeguarding concerns, relating to online challenges, scares or hoaxes – School would follow the advice in the Online Safety Policy. Prior to deciding how to respond to a harmful online challenge or hoax, the headteacher will decide whether each proposed response is: • In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes. • Careful to avoid needlessly scaring or distressing pupils. • Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils. • Proportional to the actual or perceived risk. • Helpful to the pupils who are, or are perceived to be, at risk. • Appropriate for the relevant pupils' age and developmental stage. • Supportive. • In line with the Child Protection and Safeguarding Policy. All external visitors that undertake work with children have a DBS. All visitors to school have a Visitor badge and are given a copy of the Safeguarding Leaflet. All staff complete an Induction that includes Online Safety and sign an Acceptable Use agreement, which is filed by school. There is always a member of staff who has had Accredited Safer Recruitment Training in all interviews. Visitor Safeguarding Leaflet has been updated to include Online Safety and additional DSLs.
POLICIES & PRACTICE				

Policies – do you have an online-safety policy (whether standalone or section within your safeguarding and child-protection policy? – do your policies govern all online behaviour, not just when using school devices or logged into school systems and platforms? – 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 use 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. ○ Remote learning policy (whilst covid closures are a thing of the past, remote learning systems remain in use)	🟩			School has an up-to-date stand-alone Online Safety Policy that is reviewed annually. Our school Online Safety Policy addresses online behaviour in and out of school. It includes sections on: • Cyberbullying • Peer-on-peer sexual abuse and harassment • Grooming and exploitation • Mental health • Online hoaxes and harmful online challenges • Cyber-crime • Educating parents • Remote learning ICT Acceptable Use Agreement is in place for all staff. This is signed by all staff working in school. Mobile Technologies Policy is in place. Induction Policy is in place and completed with all new starters. All staff have signed to confirm they have read KCSIE 2024. Child Protection and Safeguarding policy is in place and reviewed annually. All staff have signed to confirm they have read this policy. ECT Induction policy is in place. Employee Laptop Loan Policy is in place. School Password Management is in place. Social networking policy for staff is in place. All children sign the Think then Click Agreement, which is tailored to their phase within school (EYFS/KS1/KS2) Pupil Remote Learning Policy is in place.

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>?	🟩			Local Authority Subject Leader Updates are attended by Computing Subject leader. These meetings are used to inform changes to school Policy. Policy guidance is up to date so whenever a policy is reviewed, we can check the latest guidance is included. The policy is checked by school leaders to ensure it is current, relevant and reflects the school context. The policy is reviewed annually by a DSL and the subject leader. It is then shared with staff to review, and changes are made if necessary before it is approved by the Governing Body. A record to confirm all staff have read the policy is maintained by school in the policy file. All policies linked to Online Safety have the same clear message. Policies are updated and reflect the curriculum and school development priorities. Safeguarding risks and incidents in school are incorporated with policy guidance.
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 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**	🟩			All staff are made aware of the Online Safety expectations at their induction training. 'Online Safety- A Safeguarding Responsibility' Training Course has been attended by Dave Kirkpatrick – Assistant Head/DSL. Online Safety is now a focus within every newsletter to give advice to parents about how to keep their children safe online. This is also shared with staff across the school. Online safety trends are available through CPOMS, due to a recording tab, enabling monitoring of incidents to take place.

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?**	🟩			School responds to any national concerns relating to online safety. These are shared by the local authority through the Education Noticeboard and DSL network meetings (at least one DSL from school attends each meeting). Action: Staff to complete CPD training started last year.

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.

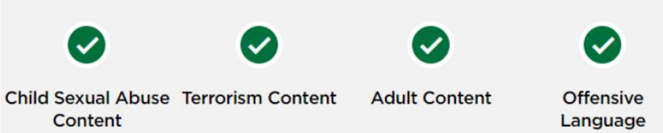
Safeguarding teams will wish to engage with their technical colleagues on this section – please ensure to review it together.

Question	**Fully In Place**	**Partial/ Needs Review**	**Not In Place**	**EVIDENCE**
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?**	🟩			Following the guidance from the Department for Education with regards to Keeping children safe in education 2024 (publishing.service.gov.uk) Our provider (Telford and Wrekin IDT Managed Services) has reviewed the Online Safety sections (page 35 onwards) and outlined how our IT Managed Service provides school with a safe environment for students and staff. Telford and Wrekin IDT Managed Services take security extremely seriously in their service offering with security being at the heart of the services they provide, along with a dedicated Security Specialist as part of their team.

Question	Fully In Place	Partial/ Needs Review	Not In Place	EVIDENCE
	🟩			Telford and Wrekin IDT Managed Services has produced a document that covers their response to the Academy trust guide to cybercrime and cyber security, the Keeping Children Safe in Education and the UK Safer Internet Checklist and for reassurance on cybercrime they have signed up to the early warning system and have done so for a number of years. They are an active member of the NCSC Cyber Information Sharing Partnership (CISP).
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?	🟩			'Online Safety- A Safeguarding Responsibility' Training Course has been attended by Dave Kirkpatrick – Assistant Head/DSL.
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?	🟩			Our Telford and Wrekin IDT use Lightspeed to block access to the following: Child Sexual Abuse Content, Terrorism, Adult Content and Offensive Language. They have used this alongside the DfE recommended testing site by SWGFL. This is up to date in line with KCSIE 2024 and the UK Safer Internet Checklist. Senso is used to filter and block inappropriate websites on all school devices. It uses Artificial Intelligence to check the content of every website a student attempts to visit and will proactively include any inappropriate websites within the filtering libraries. Senso alerts are activated and sent to the HT and DHT when any words are typed, that may be inappropriate or when inappropriate site access is attempted so that the alert can be checked and viewed in context.

Question	Fully In Place	Partial/ Needs Review	Not In Place	EVIDENCE
	🟩			Defender is used to filter emails and protect all users from spam emails. Think then Click Agreement is signed by all children in school. School Online Safety Policy includes a section on Filtering and Monitoring Online Activity. The governing board ensures the school’s ICT network has appropriate filters and monitoring systems in place. The governing board ensures ‘over blocking’ does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding. The headteacher, ICT subject leader and ICT technicians undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements are appropriate to pupils’ ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT technicians undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate. Reports of inappropriate websites or materials are made to the ICT subject leader immediately, who investigates the matter and makes any necessary changes. Deliberate breaches of the filtering system are reported to the ICT subject leader immediately, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure. If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate

Question	Fully In Place	Partial/ Needs Review	Not In Place	EVIDENCE
	🟩			agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police. The school's network and school-owned devices are appropriately monitored. All users of the network and school-owned devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the Headteacher who manages the situation in line with the Child Protection and Safeguarding Policy.
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	🟩			Senso is used to filter and block inappropriate websites on all school devices. It uses Artificial Intelligence to check the content of every website a student attempts to visit and will proactively include any inappropriate websites within the filtering libraries. Senso alerts are activated and sent to the HT and DHT when any words are typed, that may be inappropriate or when inappropriate site access is attempted so that the alert can be checked and viewed in context. Cloud based, real time monitoring of activity on school owned devices, designed to highlight to school staff users who may be vulnerable or at risk to themselves, at risk to others or behaving inappropriately. Senso indicates a potential concern by raising a "violation" when a keyword, acronym or phrase typed, matches against those found within our libraries. The violation information including a screenshot can then be viewed in the dashboard by the relevant Senso Safeguarding Portal User. The screenshot will also be analysed by our AI driven image analysis to indicate whether a student is potentially viewing harmful or inappropriate content alongside the keyword typed. This helps with prioritisation of Senso violations. T and W use the internet filtering provision: Lightspeed which blocks access to any of the material listed below

Question	Fully In Place	Partial/ Needs Review	Not In Place	EVIDENCE
	🟩			 ✓ Child Sexual Abuse Content ✓ Terrorism Content ✓ Adult Content ✓ Offensive Language If sites needed for teaching are blocked, the ICT technician can unblock these upon request if they are age appropriate. Telford and Wrekin monitor and review use regularly and will report back to school, in the event of a serious breach. Action: SENSO alerts be reviewed regularly and logged. Appropriate action will be taken as necessary.
Safe modes / search – 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?	🟩			Children cannot access YouTube in school, as access is blocked. However, teaching staff can access it to share content, as appropriate. Google safe search is enforced. Safe Searching is a critical step to keep pupils safe online.
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	🟩			All teaching staff have been provided with a Telford and Wrekin laptop that they use to access the Workgroup and their own personal workspace. Appropriate filtering and blocking is in place to avoid any inappropriate usage. Mobile phone use is not permitted in areas of school, other than the staffroom or an office. In EYFS, mobile phones are stored securely whilst staff are in the working environment.
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?	🟩			Laptops that are sent home with children are built to Telford and Wrekin Specifications by the ICT Technician. The T and W Cloud system ensures that content is filtered even when the device is not in the school building. The Headteacher continues to receive alerts, in the same way as they would if the devices were being used inappropriately in the school environment. Staff laptops, which are provided by school, also continue to be

Question	Fully In Place	Partial/ Needs Review	Not In Place	EVIDENCE
	🟩			filtered by T and W when they are connected to home Wi-Fi. Support with parental control settings and other ways parents can keep their children safe online is included in the monthly school newsletter.
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?	🟩			Online access is reviewed regularly and acted upon in an appropriate and timely manner. Alerts are checked and actioned, where appropriate by the HT or DHT. In the event of an increase in a particular area – the curriculum will be adapted or assemblies will be put in place to address safeguarding concerns. KS2 Online Behaviour Questionnaire was completed by pupils and analysed. Follow up assemblies were then put in place to address the safeguarding concerns highlighted.
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.	🟩			All staff are aware of the range of monitoring strategies that exist in school. Physical Monitoring: staff recognise the importance of monitoring pupils online use within lessons. Internet and Web Access: Staff are aware that online use is appropriately filtered, and inappropriate content is blocked by T and W. When a page that is unsuitable is accessed, it immediately loads a page saying that access is denied. No inappropriate content is displayed.
Monitoring training – 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?	🟩			Headteacher and Assistant Headteacher have met with T and W ICT Technical Support Team (Darren Booth) to pose questions about the safeguarding that is in place by the local authority to ensure that children and staff in school are unable to view unsuitable content online. 'Online Safety- A Safeguarding Responsibility' Training Course

Question	Fully In Place	Partial/ Needs Review	Not In Place	EVIDENCE
	🟩			has been attended by Dave Kirkpatrick – Assistant Head/DSL.
System configuration, customisation and review – do your technical and safeguarding teams meet to discuss your monitoring needs and ensure systems are configured for the 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?		🟧		Headteacher and Assistant Headteacher have met with T and W ICT Technical Support Team (Darren Booth) to discuss how online use is monitored across the setting through the filtering and blocking that is in place.
Reports – do you 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		🟧		Online Safety trends are monitored on CPOMS and reports are generated. Action: SENSO concerns to be logged on CPOMS, if an action is needed.
HOME / REMOTE LEARNING & DEVICES IN THE HOME				
School devices in the home – if you send school devices home with students, how are they 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?	🟩			Web Laptops that are sent home with children are built to Telford and Wrekin Specifications by the ICT Technician. The T and W Cloud system ensures that content is filtered even when the device is not in the school building. The Headteacher and Deputy Headteacher continue to receive alerts, in the same way as they would if the devices were being used inappropriately in the school environment. Support with parental control settings and other ways parents

Question	Fully In Place	Partial/ Needs Review	Not In Place	EVIDENCE
	🟩			can keep their children safe online is included in the school newsletter. School devices are locked so that no additional software can be installed. In addition, nothing on the device build can be uninstalled unless this is actioned by the technician.
Remote Learning – 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?	🟩			A remote learning policy is in place, which outlines the expectations of pupils and staff and what would happen in the event of school having to switch to remote learning for a specific reason. Safeguarding Precautions are included in the policy – see below: All teaching staff will be made aware that the procedures set out in the school's Staff Code of Conduct always apply during the delivery of remote education. Parents will be made aware of what their children are being asked to do, including: • The sites that they will be accessing. • The school staff that they will be interacting with. The DSL will arrange for regular contact to be made with vulnerable pupils during a period of remote education. Additional contact, including home visits, will be considered where required. Phone calls made to vulnerable pupils will be made using school phones where possible. All contact with vulnerable pupils will be recorded on paper and suitably stored in line with the Records Management Policy. The DSL will keep in contact with vulnerable pupils' social workers or other care professionals when the pupil is receiving remote education, as required. Vulnerable pupils will be provided with a means of contacting the DSL, their deputy, or any other relevant member of staff –

QUESTION	FULLY IN PLACE	PARTIAL/ NEEDS REVIEW	NOT IN PLACE	EVIDENCE
	🟩			this arrangement will be set up by the DSL prior to the period of remote learning. The DSL will meet (in person or remotely) with the relevant members of staff termly to discuss new and current safeguarding arrangements for vulnerable pupils learning remotely. All members of staff will report any safeguarding concerns to the DSL immediately. Pupils and their parents will be encouraged to contact the DSL if they wish to report safeguarding concerns, e.g. regarding harmful or upsetting content or incidents of online bullying. The school will also signpost families to the practical support that is available for reporting these concerns. Staff will always have due regard for the school’s Child Protection and Safeguarding Policy during remote education, e.g. whilst conducting live online lessons. The planning of live lessons will always be carried out in conjunction with the school’s DSL. The school will ensure the system used for live online lessons does not have a minimum age requirement above the age bracket of pupils attending the lesson. Pupils will not share private information through the live online system. Pupils will not respond to contact requests from people they do not know when using systems for live online lessons. Pupils will be informed of the reporting lines, should they see or hear anything inappropriate during live online lessons, via email. Pupils will be provided with the contact details of the DSL to report any concerns. Staff will ensure all video and phone calls are not set to public, and meetings are protected with passwords. Meeting links and passwords will not be published publicly.

Question	Fully In Place	Partial/ Needs Review	Not In Place	EVIDENCE
	🟩			Support staff will be on hand to supervise and handle any sudden changes or developments, such disputes between pupils, that may occur during the live online lesson. Staff will uphold their safeguarding obligations and will report any incidents or potential concerns to the DSL in line with the school's Child Protection and Safeguarding Policy. The school will ensure that parents know what pupils are expected to do for a live online lesson, including the websites pupils will be asked to use and the school staff pupils will interact with online. The school will communicate the importance of online safety to parents and encourage parents to set age-appropriate parental controls on digital devices and use internet filters to block malicious websites. The school will inform parents of the government-approved resources on child online safety to support parents further.
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?	🟩			All members of staff, including volunteers and students have to sign and agree to abide by the ICT Acceptable Use Policy.
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 allow and why, plus risks and mitigations?	🟩			ICT technical Team attends regular meetings to review online safety that is in place. School subscribes to the Gold Service and have a technician onsite once a week. ICT Technicians attend SOP meetings. The standard operating procedure (SOP) is a set of written instructions that describes the step-by-step process that must be taken to properly perform a routine activity. SOPs should be

Question	Fully In Place	Partial/ Needs Review	Not In Place	EVIDENCE
	🟩			followed the exact same way every time to guarantee that the procedures within T and W remain consistent and in compliance with industry regulations and business standards. The meeting includes a review of the roles and responsibilities of the ICT Technician.
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 pupils or between staff and pupils and that they must never use accounts/emails/apps that are not approved/linked to the school?	🟩			Online platforms used in school are limited. However, where chat functions are available, such as Teams, these are carefully monitored through SENSO and the teacher.
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?	🟩			The platforms used by pupils are included in the Homework Policy. Action: Include Learning Platforms used in school that children can access at home in the Online Safety Policy, when updated in the spring term.
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:		🟨		There is a School Emergency Plan in place with clear actions to be undertaken, in the event of a cybersecurity incident (Failure of Technology and Loss of Data Section). An inventory of all technological devices is in place and updated regularly to include new equipment.

Question	Fully In Place	Partial/ Needs Review	Not In Place	EVIDENCE
○ cybersecurity policy ○ risk + asset registers ○ incident response plan – are these accurate and regularly updated, read by all and reflected in practice? – would these answer the Ofsted *Inspecting Safeguarding* document's requirement for systems to protect against cybersecurity risks"?		🟨		
Technical staff – do technical staff have training on cybersecurity and report to senior leaders and governors on issues, mitigations incidents and training needs?	🟩			Action: Questions to explore during the cyber security conversation between the governing body and the school leaders, with governing body taking the lead. **Theme A: Information seeking** Factual questions by the governing body to give the school a good understanding of their ICT estate: 1. **Does the school have a list of the different organisations that provide its ICT services?** School subscribes to the Telford and Wrekin Gold Service for ICT support. The range of programs we use are vetted by T and W and listed on the subscriptions list managed by the school business manager. All programmes have been explored and vetted by school staff to ensure online safety. Online learning platforms that can be accessed from home are included in the online safety policy.

Question	Fully In Place	Partial/ Needs Review	Not In Place	EVIDENCE
	🟩			**2. Does the school leader know who manages or coordinates the ICT within the school?** Julie Thornton – liaises with ICT technician, manages ICT budget, co-ordinates website, generates passwords and all technical issues Gemma Gill-Computing lead Dave Kirkpatrick- DSL with online safety responsibility Julie Thornton- Manages subscriptions and list of programs used **3. Has the school identified the most critical parts of the school's digital estate and sought assurance about its security?** School adheres to cyber security best practices when buying in Telford and Wrekin ICT services and the ICT technician comes in weekly and liaises with Lisa Lloyd. Internet filtering system- Defender firewall SENSO- allows senior leaders to monitor ICT activity and malpractice Regular feedback is given to governors via Health and Safety committee and full governing body meetings. **4. Does the school have a proper backup and restoration plan in place?** **Yes, it is backed up - linked to Abraham Darby.** Moved to Sharepoint 365 where everything is saved to the

QUESTION	FULLY IN PLACE	PARTIAL/ NEEDS REVIEW	NOT IN PLACE	EVIDENCE
	🟩			cloud and easily accessible. **Theme B: Awareness** The degree to which both users and the governing body understand the importance of cyber security and their role in it: **5. Do the school's governance and ICT policies reflect the importance of good cyber security?** An online safety policy is in place (Reviewed March 23) which includes sections on filtering and monitoring online activity and network security. Section 16 and 17. "Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians. Firewalls are switched on at all times. ICT technicians review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates. Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments and are expected to report all malware and virus attacks to ICT technicians." **6. Does the school train staff on the common cyber security threats and incidents that schools experience?** At every staff or governor meeting, there is an item on safeguarding that is often linked to online safety. Computing lead attends termly computing update DSL with online safety attended Online Safety-a Safeguarding Responsibility Messages from these discussed in SLT meetings and fed back to

Question	Fully In Place	Partial/ Needs Review	Not In Place	EVIDENCE
	🟩			staff and governors. **Theme C: Preparedness** Being prepared for the potential impact of a cyber security incident is crucial in helping schools minimise disruption should an incident occur: **7. If the school temporarily lost access to its data and/or internet connection would the school still be able to operate?** Yes – staff can adapt quickly in these situations. **8. Does the school know who to contact if it becomes a victim of a cyber incident?** The school emergency plan details what to do in the event of a cyber security incident . Section 10 page 48-49 The NCSC questions for governors document may be helpful here – ncsc.gov.uk/information/school-governor-questions
Training – are non-technical staff given training and regular reminders on cybersecurity best-practice (passwords, phishing, reporting and more)?	🟩			Safeguarding updates are shared weekly at the start of every staff meeting and email reminders from Rob Montgomery.