

# ***The Ryde School***

## ***Online Safety Policy***



Reviewed: September 2025  
Next Review: September 2027



# Contents

1. Introduction.....	3
2. Responsibilities.....	3
3. Scope of policy.....	3
4. Monitoring and Filtering.....	4
5. Policy and procedure .....	4
Use of email .....	5
Visiting online sites and downloading .....	5
Storage of Images .....	6
Use of personal mobile devices (including phones) .....	7
New technological devices .....	8
Reporting incidents, abuse and inappropriate material .....	8
6. Curriculum .....	8
7. Staff and Governor Training.....	9
8. Working in Partnership with Parents/Carers.....	9
9. Records, monitoring and review.....	10
10. Appendices of the Online Safety Policy.....	10
Appendix A -Online Safety Acceptable Use Agreement - Staff ,Governors,student teachers .....	11
Appendix B - Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches and supply teachers.....	14
Appendix C - Requirements for visitors, volunteers and parent/carers helpers .....	17
Appendix D - Online Safety Acceptable Use Agreement Primary Pupils .....	18
Appendix E - Online Safety Acceptable Use Agreement Secondary Pupils .....	20
Appendix F - Online safety policy guide - Summary of key parent/carers responsibilities .....	21
Appendix G - Guidance on the process for responding to cyberbullying incidents .....	22
Appendix H - Guidance for staff on preventing and responding to negative comments on social media.....	23
Appendix I - Online safety incident reporting form.....	25
Appendix J - Online safety incident record.....	27
Appendix K - Online safety incident log.....	29
Appendix L - Safeguarding and remote education during coronavirus (COVID-19) Useful resources .....	30
Appendix M – Annual Online Safety Audit Template .....	31

## 1. Introduction

The Ryde School recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** pupils, staff and governors will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

## 2. Responsibilities

The headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety lead in this school is Sue Thompson.

All breaches of this policy must be reported to Sue Thompson.

All breaches of this policy that may have put a child at risk must also be reported to a DSP..

Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, cloud-based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when pupils are on site in the care of the school, then the safeguarding of pupils is paramount and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

## 3. Scope of policy

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe

online.

The school provides online safety information for parents/carers, for example, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: safeguarding, Keeping Children Safe in Education, GDPR, health and safety, home–school agreement, behaviour, anti-bullying and PSHCE/RSE policies.

#### **4. Filtering and Monitoring**

Responsibilities:

Ensuring that standards are met:

Governor: Rosemary Ramsdale

Headteacher: Sue Thompson

Responsibility for filtering and monitoring:

IT Curriculum Co-ordinator: Catherine Brumby

External Service Provider: InTermIT

All responsibilities and technical requirements to meet the standard will be adhered to as clarified in the DfEs document 'Meeting Digital and Technology Standards in Schools and Colleges'. <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges>

The school will conduct a review of the filtering and monitoring system at least annually. The deputy headteacher, curriculum lead and external service provider will conduct this review and report the outcomes to the headteacher and link governor. See **Appendix M**

#### **5. Policy and procedure**

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

## Use of email

Staff and governors should use a school email account or Governor Hub for all official school communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address. Pupils should use school approved accounts on the school system for educational purposes. Where required parent/carer permission will be obtained for the pupil account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the policy for GDPR. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors and pupils should not open emails or attachments from suspect sources and should report their receipt to Sue Thompson.

**Users must not** send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

## Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service and seek approval from a senior leader. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required. If internet research is set for homework, specific sites will be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources.
- Staff must only use pre-approved systems if creating blogs, wikis or other online content.
- When working with pupils, searching for images should be done through Google Safe Search (standard through the HICS service), Google Advanced Search or a similar application that provides greater safety than a standard search engine.

### **Users must not:**

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)

- Adult material that breaches the Obscene Publications Act in the UK
- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation
- Promoting hatred against any individual or group from the protected characteristics above
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

**Users must not:**

- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

Only a school device may be used to conduct school business outside of school. The only exception would be where a closed, monitorable system has been set up by the school for use on a personal device. Such a system would ensure the user was not saving files locally to their own device and breaching data security.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by Sue Thompson.

Storage of Images

Photographs and videos provide valuable evidence of pupils' achievement and

progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud based services. Rights of access to stored images are restricted to approved staff as determined by Sue Thompson. Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. See also GDPR. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

#### Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of pupils. Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from Sue Thompson. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

Pupils are allowed to bring personal mobile devices/phones to school but they must be switched off and stored in the school office during school hours. Under no circumstance should pupils use their personal mobile devices/phones to take images of

- any other pupil unless they and their parents have given agreement in advance
- any member of staff

The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Personal mobiles, belonging to either staff or pupils, must never be used to access school emails and data. The only exception would be where a closed, monitorable system has been set up by the school for use on a personal device.

### New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with SueThompson before they are brought into school.

### Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the DSP or the headteacher. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSP will refer details to social care or the police.

## **6. Curriculum**

Online safety is fully embedded within our curriculum. The school provides a comprehensive age appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation. The PSHE curriculum, Relationships and Health Curriculum are central in supporting the delivery of online safety education.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment
- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online
- Thinking carefully before placing images online and considering their



appropriateness and understanding the importance of gaining consent before posting photographs of others

- Understanding the permanency of all online postings and conversations

Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.

- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.
- How the law can help protect against online risks and abuse

## **7. Staff and Governor Training**

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with pupils.

Any organisation working with children and based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement (Appendix B).

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (Appendix B).

Guidance is provided for occasional visitors, volunteers and parent/carers helpers.

## **8. Working in Partnership with Parents/Carers**

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.

It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and by other means.

Parents/carers are required on a biannual basis (in classes Y1, Y3 and Y5) to read, discuss and co-sign with each child the Acceptable Use Agreement. New starters will also be required read, discuss and co-sign the Acceptable Use Agreement with their parents/carers.

## **9. Records, monitoring and review**

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes. In addition governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

## **10. Appendices of the Online Safety Policy**

- A. Online Safety Acceptable Use Agreement - Staff, Governors and student teachers (on placement or on staff)
- B. Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers
- C. Requirements for visitors, volunteers and parent/carers helpers working in the school (working directly with children or otherwise)
- D. Online Safety Acceptable Use Agreement Primary Pupils
- E. Online Safety Acceptable Use Agreements Secondary Pupils
- F. Online safety policy guide - Summary of key parent/carer responsibilities
- G. Guidance on the process for responding to cyberbullying incidents
- H. Guidance for staff on preventing and responding to negative comments on social media
- I. Online safety incident reporting form
- J. Online safety incident record
- K. Online safety incident log
- L. Safeguarding and remote education during coronavirus
- M. Annual Online Safety Audit

## **Appendix A - Online Safety Acceptable Use Agreement - Staff, Governors and student teachers (on placement or on staff)**

You must read this agreement in conjunction with the online safety policy and the GDPR policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff, student teachers and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with Sue Thompson. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

### **Internet Access**

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSP and an incident report completed.

### **Online conduct]**

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Sue Thompson.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

### **Social networking**

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

When using social networking for personal use I will endeavour to ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

## **Passwords**

I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

## **Data protection**

I will follow requirements for data protection as outlined in GDPR policy. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely
- Personal data can only be taken out of school or accessed remotely when authorised by the headteacher or governing body
- Personal or sensitive data taken off site must be encrypted

## **Images and videos**

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.

## **Use of email**

I will use my school email address or governor hub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my school email addresses or governor hub for personal matters or non-school business.

## **Use of personal devices**

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

I will only use approved personal devices in designated areas and never in front of pupils.

I will not access secure school information from personal devices when in school or any other location unless a closed, monitorable system has been set up by the school. Such a system would ensure as the user I was not saving files locally to my own device and breaching data security.

## **Additional hardware/software**

I will not install any hardware or software on school equipment without permission of Sue Thompson.

## **Promoting online safety**

I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, pupils or parents/carers) to a DSP or Sue Thompson.

### **Classroom management of internet access**

I will pre-check for appropriateness all internet sites used in the classroom this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils. I will also check the appropriacy of any suggested sites suggested for home learning.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with Sue Thompson.

### **Video conferencing**

I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DPO and DSP. A school-owned device should be used when running video-conferences, where possible.

### **User signature**

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

## **Appendix B - Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers**

**School name: The Ryde School**

**Online safety lead: Sue Thompson**

**Designated Safeguarding Lead (DSL) Sue Thompson**

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with Sue Thompson. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The school's online safety policy will provide further detailed information as required.

### **Internet Access**

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSP and an incident report completed.

### **Online conduct**

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Sue Thompson.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with Sue Thompson.

### **Social networking**

I understand the need to separate my professional role from my private friendships; in my professional

capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

Information can be shared with pupils over 13 and parents/carers through an organisational social network site/page e.g. on Facebook or Twitter, but never through a personal account or site. In my professional role in the school, I will never engage in 1-1 exchanges with pupils or parent/carers on personal social network sites.

My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information known as a result of my work in the school must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

### **Passwords**

I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

### **Data protection**

I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs and videos. Once agreed, these must be made on a school device.
- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

### **Images and videos**

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose or, in the case of 1:1 tuition, pupil's or parent/carer devices can be used, with parent/carer agreement.

Internet, mobile and digital technologies provide helpful recording functions but these cannot be made on a teacher's personal device. Recordings can be made with the child's and parent/carer's agreement on a school device, an organisational device approved by the headteacher/DSP, or a young person's or parent/carer's own device.

### **Use of Email**

I will only use my professional email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters.

### **Use of personal devices**

I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I

understand that the use of personal devices in school is at the discretion of the headteacher.

I will only use approved personal devices in designated areas and never in front of pupils. This therefore precludes use of specialist apps on personal devices. A school device could be used to access specialist apps that support pupil learning. Pupils can also be encouraged, but not required, to access such apps on their own devices if allowed by the school and with parent/carers agreement.

### **Additional hardware/software**

I will not install any hardware or software on school equipment without permission of Sue Thompson.

### **Promoting online safety**

I understand that online safety is part of my responsibility and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, governors, visitors, pupils or parents/carers) which I believe may be inappropriate or concerning in any way to the DSP or Sue Thompson.

### **Classroom management of internet access**

I will pre-check for appropriateness all internet sites used in the classroom or during a tutoring session; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with Sue Thompson.

### **Video conferencing**

I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DPO and DSP. A school-owned device should be used when running video-conferences, where possible.

### **User Signature**

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature ..... Date .....

Full Name ..... (Please use block capitals)

Job Title/Role .....



## **Appendix C - Requirements for visitors, volunteers and parent/carers helpers (Working directly with children or otherwise)**

**School name: The Ryde School**

**Online safety lead: Sue Thompson**

**DSL: Sue Thompson**

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise **any** safeguarding concerns arising from your visit immediately with the headteacher and/or DSP

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.
- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.
- I will not give out my personal details such as mobile phone number, email address, and social media account details to pupils. Where appropriate I may share my professional contact details with parents/carers provided the DSP or headteacher is informed before I leave the school.
- I understand my visit to the school may give me access to privileged information about pupils, staff, school systems and plans. Such information should never be shared on line, including on social media sites.
- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the headteacher.
- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of pupils. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school.

Signed:

## Appendix D - Online Safety Acceptable Use Agreement Primary Pupils

### My online safety rules

- I will only use school IT equipment for activities agreed by school staff.
- I will not use my personal email address or other personal accounts in school
- I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher and agreed by my parent/carer.
- I will only open email attachments if it has been approved by a member of school staff in school or a parent/carer out of school.
- In school I will only open or delete my files when told by a member of staff.
- I will not tell anyone other than my parents/carers my passwords. I will not use other people's usernames or passwords to pretend to be them online.
- I will make sure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.
- If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or my parent/carer immediately.
- If someone says, asks or posts about me anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will not reply. I will tell my teacher or my parent/carer immediately.
- I will not give out my own or other people's personal information, including: name, phone number, home address, interests, schools or clubs. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parent's/carer's permission.
- Even if I have permission, I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- I understand that some people on the internet are not who they say they are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.
- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.
- I understand that some personal devices are allowed in school and some are not, and I will follow the rules. I will not assume that new devices can be brought into school without getting permission.
- I understand my behaviour in the virtual classroom should mirror that in the physical classroom
- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.

- I understand that these rules are designed to keep me safe now and in the future. If I break the rules my teachers will look into it and may need to take action.

Please return the signed sections of this form which will be kept on record at the school.

### **Pupil agreement**

Pupil name.....

This agreement is to keep me safe. I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Pupil signature.....

### **Parent(s)/Carer(s) agreement**

Parent(s)/Carer(s) name(s).....

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child/ren. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or post material that may bring the school or any individual within it into disrepute.

(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents).

Parent/carer signature.....

Date .....

## **Appendix F - Online safety policy guide - Summary of key parent/carers responsibilities**

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for pupils.
- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carers is on school premises but not in a designated area, their phone/s must be switched off and out of sight.
- Parents/carers should not assume that pupils can bring technological devices to school and should always check the school policy.
- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.
- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.
- Any parent/carers, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents/carers.

Please see the full online safety policy in the policies section on the school website.

## **Appendix G - Guidance on the process for responding to cyberbullying incidents**

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, headteacher) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the headteacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

## **Appendix H - Guidance for staff on preventing and responding to negative comments on social media**

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy, see especially Appendix F (Online safety policy guide - Summary of key parent/carer responsibilities), clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

- Collect the facts

As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the police and the headteacher will need to follow the school's safeguarding procedures.

If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

- Addressing negative comments and complaints

Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

The meeting must:

- Draw attention to the seriousness and impact of the actions/postings;
- Ask for the offending remarks to be removed;
- Explore the complainant's grievance;
- Agree next steps;
- Clarify the correct complaints procedures.

If the meeting does not resolve the issue, the parents must be informed that the school will

need to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law;
- Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.

## Appendix I - Online safety incident reporting form

Any member of the school community can raise a concern about an online safety incident. If you have witnessed or experienced an incident, please complete the form below to help us to address the issue. It is important that you provide as much detail as possible. Once completed please hand this report to Sue Thompson.

Name of person reporting incident:			
Signature:			
Date you are completing this form:			
Where did the incident take place:	Inside school?		Outside school?
Date of incident(s):			
Time of incident(s):			

Who was involved in the incident(s)?	Full names and/or contact details
Children/young people	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyber bullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of acceptable use agreement, please specify			



Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence available but do not attach.

**Thank you for completing and submitting this form.**

## Appendix J - Online safety incident record

Name of person reporting incident:			
Date of report:			
Where did the incident take place:	Inside school?		Outside school?
Date of incident(s):			
Time of incident(s):			

Who was involved in the incident(s)?	Full names and/or contact details
Children/young person	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyberbullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of Acceptable Use Agreement			
Other, please specify			

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence provided but do not attach

Immediate action taken following the reported incident:	
Incident reported to online safety Lead /DSP/ /Headteacher	
Safeguarding advice sought, please specify	
Referral made to HCC Safeguarding	
Incident reported to police and/or CEOP	
Online safety policy to be reviewed/amended	
Parent(s)/carer(s) informed please specify	
Incident reported to social networking site	
Other actions e.g. warnings, sanctions, debrief and support	
Response in the wider community e.g. letters, newsletter item, assembly, curriculum delivery	

<b>Brief summary of incident, investigation and outcome (for monitoring purposes)</b>	
---	--

## Appendix K - Online safety incident log

Summary details of ALL online safety incidents will be recorded on this form by the online safety lead or other designated member of staff. This incident log will be monitored at least termly and information reported to SLT and governors.

Date & time	Name of pupil or staff member Indicate target (T) or offender (O)	Nature of incident(s)	Details of incident (including evidence)	Outcome including action taken

## **Appendix L – Safeguarding and remote education during coronavirus (COVID-19)**

### **Useful resources**

Below are resources (please note not an exhaustive list) to help schools manage and risk assess any remote teaching and working.

#### **Government guidance on safeguarding and remote education**

<https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19>

#### **The Key for School Leaders - Remote learning: safeguarding pupils and staff**

<https://schoolleaders.thekeysupport.com/covid-19/safeguard-and-support-pupils/safeguarding-while-teaching/remote-teaching-safeguarding-pupils-and-staff/?marker=content-body>

#### **NSPCC Undertaking remote teaching safely**

<https://learning.nspcc.org.uk/news/2020/march/undertaking-remote-teaching-safely>

#### **LGfL Twenty safeguarding considerations for lesson livestreaming**

<https://static.lgfl.net/LgflNet/downloads/digisafe/Safe-Lessons-by-Video-and-Livestream.pdf>

#### **swgfl Remote working a guide for professionals**

<https://swgfl.org.uk/assets/documents/educational-professionals-remote-working.pdf>

#### **National Cyber Security Centre Video conferencing. Using services securely**

[https://www.ncsc.gov.uk/files/vtc\\_infographic.pdf](https://www.ncsc.gov.uk/files/vtc_infographic.pdf)

## Appendix M – Annual Online Safety Audit

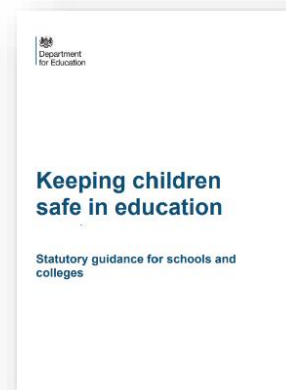


# Annual School Online Safety Audit & Risk Assessment

According to Keeping Children Safe in Education, “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 tickbox 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, emphasis added).



This isn't just about the education/curriculum side though – KCSIE 2022 also includes a new mention of school leaders (not technicians) regularly reviewing systems' effectiveness, and that's why we start the audit with the Safe School Systems section. Please note that we have given a little more detail in this section than in the education section to help non-technical colleagues better understand technical issues. The length does not reflect relative importance to education and messaging.

We recommend that results, conclusions and actions are incorporated into a 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)

We suggest you use the final column to add the evidence, links, details and when it was checked, plus risks and actions/mitigations (by way of documenting your risk assessment).

Feel free to edit this template and add your school logo but please do not remove the LGfL branding or copyright notice and rather than share the file, if you would like to share with other schools, ask them to visit [onlinesafetyaudit.lgfl.net](https://onlinesafetyaudit.lgfl.net)

Remember to share results with your school governors or trustees to help them fulfil their oversight duties. We welcome feedback to help us improve the tool, via [safeguarding@lgfl.net](mailto:safeguarding@lgfl.net)

## 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	<ul style="list-style-type: none"> <li>Evidence / details and dates</li> <li>Any actions / by whom?</li> <li>Add <b>colour highlights</b> for items to add to risk register</li> </ul> <p><i>NB – we pre-filled examples / links – delete as appropriate</i></p>
APPROACH				
<p><b>Approach: whole-school &amp; safeguarding-driven</b></p> <ul style="list-style-type: none"> <li>– 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?</li> <li>– 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?</li> <li>– 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?</li> <li>– is online safety included on safeguarding reports?</li> <li>– does online safety have obvious involvement of the leadership team and governors?</li> <li>– how does the school ensure that non-specialist staff use consistent approaches and messaging?</li> <li>– 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)?</li> </ul>				<p>It may be helpful to reference <a href="https://www.gov.uk/government/publications/teaching-online-safety-in-schools">https://www.gov.uk/government/publications/teaching-online-safety-in-schools</a></p>
<p><b>Approach: flexible, current curriculum</b></p> <ul style="list-style-type: none"> <li>– 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)?</li> <li>– are staff comfortable with making the most of ad hoc opportunities to discuss and learn as online safety conversations arise?</li> <li>– how does the school review annually that teaching is current and relevant to the setting and pupil needs and experiences?</li> </ul>				<p>You may wish to reference/consult:</p> <ul style="list-style-type: none"> <li><a href="https://www.gov.uk/government/publications/teaching-online-safety-in-schools">https://www.gov.uk/government/publications/teaching-online-safety-in-schools</a></li> <li><a href="https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education">https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education</a></li> <li><a href="https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study">https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study</a></li> </ul>

<ul style="list-style-type: none"> <li>– are all the harms and issues and ‘underpinning behaviours’ mentioned in TOSIS and the RSHE guidance addressed throughout the year?</li> <li>– is particular consideration made for vulnerable students, e.g. those with SEND and other needs?</li> <li>– how does the school avoid overlapping teaching, e.g. covering the same issue in different subjects (e.g. RSHE and Computing)?</li> <li>– do you collate ‘pupil voice’ to ensure messaging addresses pupils’ lived experiences?</li> <li>– do you ensure that positive experiences online are also celebrated (not just harms and negative aspects of life online)?</li> </ul>				
<b>Assessment</b> <ul style="list-style-type: none"> <li>– is the curriculum informed by and measured against clear outcomes, e.g. those in the UKCIS framework Education for a Connected World (or similar)?</li> <li>– 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</li> </ul>				<p>Education for a Connected World is available at <a href="https://gov.uk/government/publications/education-for-a-connected-world">gov.uk/government/publications/education-for-a-connected-world</a></p> <p>The SafeSkills online safety quiz tool is free for all UK schools to use and includes teacher stats <a href="https://safeskills.lgfl.net">safeskills.lgfl.net</a></p>
<b>Parental engagement</b> <ul style="list-style-type: none"> <li>– how do you proactively engage parents/carers?</li> <li>– are parents aware of the school’s broad online-safety approach?</li> <li>– 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?</li> <li>– are parents reminded of the importance of following age ratings?</li> <li>– do you follow a drip-feed approach to communicating with parents?</li> </ul>				<p>Resources from <a href="https://parentsafe.lgfl.net">parentsafe.lgfl.net</a> may be helpful here and <a href="https://scare.lgfl.net">scare.lgfl.net</a></p>
<b>External influences, resources and scares</b> <ul style="list-style-type: none"> <li>– are external resources always first assessed for appropriateness (age appropriate, not overly negative, scary, victim blaming etc)?</li> <li>– are any external purchased schemes of work/curricula carefully adapted as necessary?</li> <li>– what approach does the school take to reacting to online challenges, scares and hoaxes?</li> <li>– how are any external visitors vetted for expertise, appropriateness and safeguarding understanding?</li> </ul>				<p>It may be helpful to reference</p> <ul style="list-style-type: none"> <li>• <a href="https://scare.lgfl.net">scare.lgfl.net</a></li> <li>• <a href="https://gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes">gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes</a></li> <li>• UKCIS victim-blaming guidance (<i>soon to be published at time of publication of this document</i>)</li> <li>• <a href="https://gov.uk/government/publications/using-external-visitors-to-support-online-safety-education-guidance-for-educational-settings">gov.uk/government/publications/using-external-visitors-to-support-online-safety-education-guidance-for-educational-settings</a></li> </ul> <p>LGfL provides signposting to a range of themed resources at <a href="https://saferesources.lgfl.net">https://saferesources.lgfl.net</a></p>
<b>POLICIES &amp; PRACTICE</b>				
<b>Policies</b> <ul style="list-style-type: none"> <li>– do your policies govern all online behaviour, not just when using school devices or logged into school systems and platforms?</li> </ul>				<p>Several organisations provide customisable templates, including LGfL at <a href="https://safepolicies.lgfl.net">https://safepolicies.lgfl.net</a></p>



<ul style="list-style-type: none"> <li>– do you have an online-safety policy (whether standalone or section within your safeguarding and child-protection policy?</li> <li>– do you have (note the following might be integrated into other policies and not standalone but must be very clear if so) <ul style="list-style-type: none"> <li>○ 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).</li> <li>○ Social media policy? If not, this may be included in your online safety policy but should be clear.</li> <li>○ Remote learning policy (whilst covid closures are a thing of the past, remote learning systems remain in use)</li> </ul> </li> </ul>				
<p><b>Content &amp; review, policy v. practice</b></p> <ul style="list-style-type: none"> <li>– do you consult others to populate your policy, e.g. review templates (LSCP, fellow schools, The Key, LGfL, etc)?</li> <li>– where you have used content or templates, have you checked it is relevant to your setting, systems and stakeholders and adapted as appropriate?</li> <li>– do you regularly review these policies (not just the annual governor review but with staff and pupils who can give insights into practicability)?</li> <li>– 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)?</li> <li>– are new systems, platforms, processes and user behaviour/needs regularly incorporated into these ‘living’ documents?</li> <li>– are policies updated to reflect curriculum needs, behaviour and safeguarding risks and incidents <u>in your school</u>?</li> </ul>				
<h2>TRAINING</h2>				
<p><b>Training &amp; CPD</b></p> <ul style="list-style-type: none"> <li>– 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)?</li> <li>– is the centre of expertise in online safety within the DSL team with the most in-depth training received by this team?</li> <li>– are regular updates given throughout the year, reflecting trends, harms and incidents in school as</li> </ul>				<p>Free training is available from LGfL at <a href="https://safetraining.lgfl.net">safetraining.lgfl.net</a>  And from most LSCPs (Local Safeguarding children Partnerships)  Excellent paid training is available from many organisations such as NSPCC.</p>

<p>well as nationally?</p> <ul style="list-style-type: none"> <li>– is training appropriate to and customised for different roles and responsibilities, with extra strategic elements for SLT and governors?</li> <li>– 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)?</li> <li>– do technical staff receive sufficient training on key safeguarding elements?</li> <li>– do non-technical staff receive sufficient training on technical aspects?</li> </ul>				
--	--	--	--	--

[ END OF SECTION 1 ]

## 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	<ul style="list-style-type: none"> <li>Evidence / details and dates</li> <li>Any actions / by whom?</li> <li>Add <b>colour highlights</b> for items to add to risk register</li> </ul> <i>NB – we pre-filled examples / links – delete as appropriate</i>
<b>FILTERING</b>				
<b>Appropriate filtering</b> <ul style="list-style-type: none"> <li>– has your provider filed a submission with the UK Safer Internet Centre to explain why your filtering is 'appropriate'?</li> <li>– 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?</li> </ul>				Safer Internet Centre submissions - <a href="https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/filtering-provider-responses">https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/filtering-provider-responses</a>  YouTube guidance - <a href="https://youtube.lgfl.net">https://youtube.lgfl.net</a>
<b>Filtering training</b> <ul style="list-style-type: none"> <li>– 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?</li> <li>– 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?</li> </ul>				Tech training - <a href="https://lgfl.bookinglive.com/book/add/p/23">https://lgfl.bookinglive.com/book/add/p/23</a>  Safeguarding training (20 minute overview) - <a href="https://lgfl.bookinglive.com/book/add/p/5">https://lgfl.bookinglive.com/book/add/p/5</a>
<b>Rationale / team effort</b> <ul style="list-style-type: none"> <li>– 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?</li> <li>– 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?</li> </ul>				
<b>Reporting and regular review</b> <ul style="list-style-type: none"> <li>– 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 &amp;</li> </ul>				e.g. Viewing top blocked sites / categories monthly will highlight trends and changes that need to be investigated or addressed by talking to students.

<p>learning sites)?</p> <ul style="list-style-type: none"> <li>– who is responsible for checking these reports have been run and are being reviewed, and that they are functioning correctly?</li> <li>– is the system regularly reviewed to ensure appropriate access, settings and usage, including consideration of impact</li> </ul>				
<p><b>Safe modes / search</b></p> <ul style="list-style-type: none"> <li>– 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?</li> </ul>				<p>YouTube mode checked via <a href="https://youtubemode.lgfl.net">https://youtubemode.lgfl.net</a></p> <p>YouTube settings overview at <a href="https://youtube.lgfl.net">https://youtube.lgfl.net</a></p> <p>Check at the top right of the search page if Google safe search is enforced (LGfL schools request this via a DNS change)</p>
<p><b>BYOD</b></p> <ul style="list-style-type: none"> <li>– 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</li> </ul>				<p>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</p>
<p><b>Devices at home</b></p> <ul style="list-style-type: none"> <li>– have you applied filtering to school devices when sent home with students?</li> <li>– given that schools cannot protect parent/child devices, do you remind parents about how to set controls on their home internet/phones/devices etc?</li> </ul>				<p>Web filtering for school devices at home is available from various providers including LGfL – those solutions which also have Chrome extensions can also protect children if they access a school profile on a family device</p> <p>See <a href="https://parentsafe.lgfl.net">https://parentsafe.lgfl.net</a> for support with parental control settings and other ways parents can keep their children safe online</p>
<p><b>Linked to the curriculum and safeguarding landscape</b></p> <ul style="list-style-type: none"> <li>– is your filtering set up and updated to reflect the online-safety messages you teach and safeguarding concerns/cases in school?</li> <li>– conversely, is learning from filtering findings used to inform the curriculum?</li> </ul>				<p>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?</p>
<b>MONITORING</b>				
<p><b>Approach</b></p> <ul style="list-style-type: none"> <li>– is your approach to monitoring based on a strategic and safeguarding-driven rationale that has been made in discussion between safeguarding and technical teams?</li> <li>– 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.</li> </ul>				<p>Safer Internet Centre monitoring approaches - <a href="https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-monitoring">https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-monitoring</a></p>
<p><b>Appropriate monitoring</b></p> <ul style="list-style-type: none"> <li>– if you use a pro/active technical monitoring solution, has the provider filed a submission to the UK Safer Internet Centre?</li> <li>– have DSL, SLT and technical teams all read and understood this submission, including rationale, benefits and limitations.</li> </ul>				<p>Safer Internet Centre appropriate monitoring provider submissions – <a href="https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/monitoring-providers-responses">https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/monitoring-providers-responses</a></p>
<b>Monitoring training</b>				

<ul style="list-style-type: none"> <li>– 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?</li> <li>– 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?</li> </ul>				
<b>System configuration, customisation and review</b> <ul style="list-style-type: none"> <li>– 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?</li> <li>– 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.</li> <li>– 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?</li> </ul>				
<b>Reports</b> <ul style="list-style-type: none"> <li>– 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?</li> <li>– do you also run reports to spot trends over time?</li> <li>– 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?</li> </ul>				
<b>Other</b> <ul style="list-style-type: none"> <li>– 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.</li> </ul>				
<b>HOME / REMOTE LEARNING &amp; DEVICES IN THE HOME</b>				
<b>School devices in the home</b> <ul style="list-style-type: none"> <li>– if you send school devices home with students, how are they protected / monitored?</li> <li>– do you have internet filtering/monitoring on them?</li> <li>– are they locked down as ‘managed devices’ so software cannot be un/installed except by school</li> </ul>				<p>Web filtering for school devices at home is available from various providers including LGfL.</p>

admins?				
<b>Live lessons</b> (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?				The infographic at <a href="https://remotesafe.lgfl.net">https://remotesafe.lgfl.net</a> 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.
<b>Homework / cloud platforms accessible from home</b> (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?				
<b>GENERAL – ALL TECHNOLOGY USED IN / BY THE SCHOOL</b>				
<b>Safeguarding &amp; technical collaboration and review</b> – 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?				State here where this review document is kept and its latest update
<b>Communication functionality</b> – 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?				
<b>Technology in your policies / AUPs</b> – are the latest school system, platforms and devices that <b>CAN</b> 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)?				See <a href="https://safepolicies.lgfl.net">safepolicies.lgfl.net</a> for template policies  Consider asking staff and students what they think of policies, not just if they agree
<b>CYBERSECURITY</b>				

<p><b>Audit &amp; documentation</b> (given its importance for continuity of access to systems and data for keeping children safe, schools secure and maintaining continuity of teaching &amp; learning, cybersecurity should be audited separately)</p> <ul style="list-style-type: none"> <li>– does your school have the recommended 3 documents from the NCSC: <ul style="list-style-type: none"> <li>o cybersecurity policy</li> <li>o risk + asset registers</li> <li>o incident response plan</li> </ul> </li> <li>– are these accurate and regularly updated, read by all and reflected in practice?</li> <li>– would these answer the Ofsted <i>Inspecting Safeguarding</i> document's requirement for systems to protect against cybersecurity risks?"</li> </ul>				<p>Templates for these three documents including notes to explain to a non-technical audience are at <a href="https://elevate.lgfl.net">https://elevate.lgfl.net</a></p>
<p><b>Technical staff</b></p> <ul style="list-style-type: none"> <li>– do technical staff have training on cybersecurity and report to senior leaders and governors on issues, mitigations incidents and training needs?</li> </ul>				<p>The NCSC questions for governors document may be helpful here – <a href="https://ncsc.gov.uk/information/school-governor-questions">ncsc.gov.uk/information/school-governor-questions</a></p>
<p><b>Training</b></p> <ul style="list-style-type: none"> <li>– are <u>non-technical</u> staff given training and regular reminders on cybersecurity best-practice (passwords, phishing, reporting and more)?</li> </ul>				<p>NCSC non-technical training for school staff is available for free, e.g. from LGfL <a href="https://booking.lgfl.net/book/add/p/33">https://booking.lgfl.net/book/add/p/33</a></p>

