360safe.org.uk
360safe@swgfl.org.uk

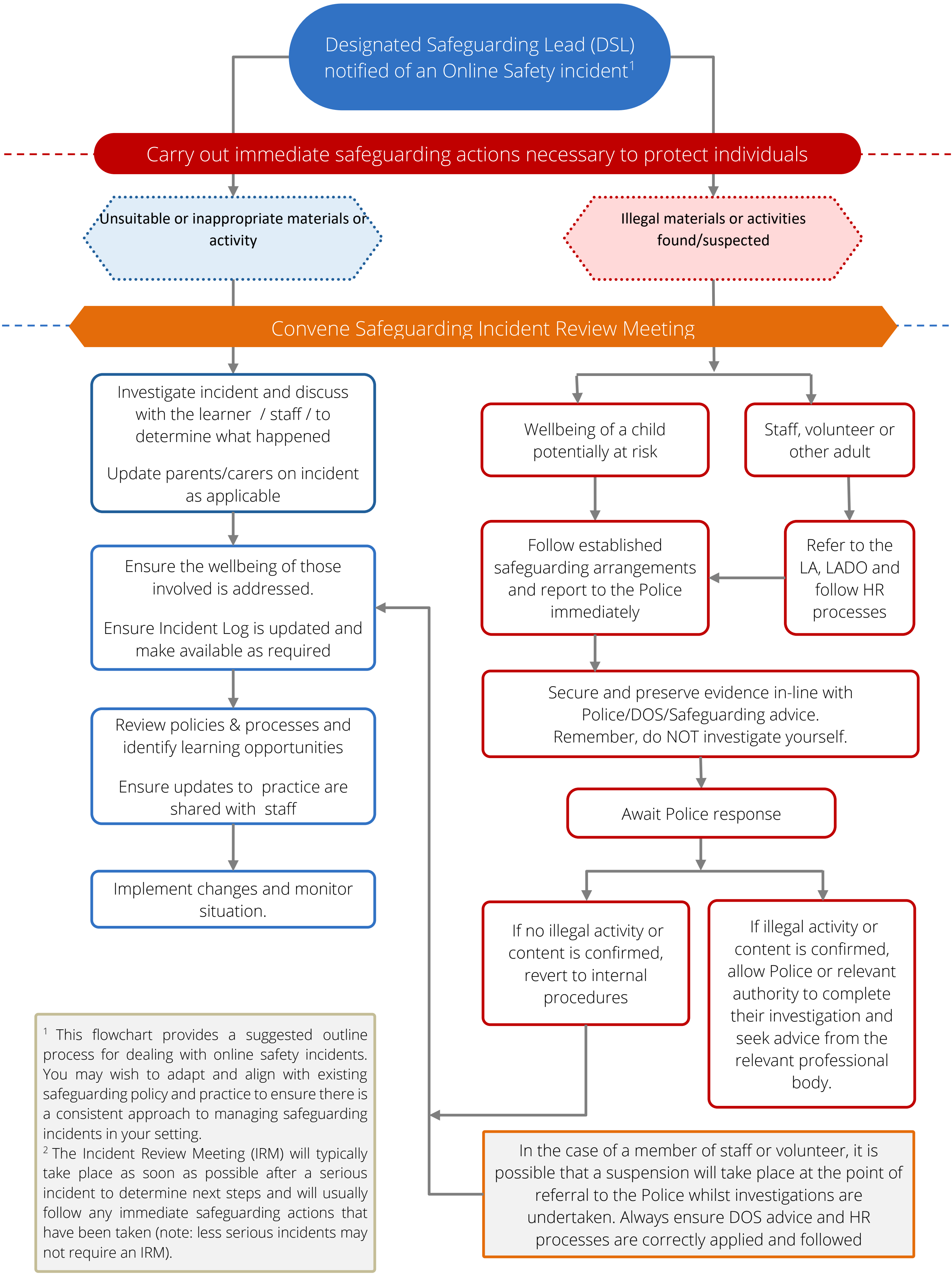
User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. The National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways– further information here					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright and intellectual property (including through the use of AI services)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Consideration should be given for the following activities when undertaken for non-educational purposes:	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/
Online gaming								
Social media including messaging/chat								
Entertainment streaming e.g. Netflix, Disney+								
Use of video broadcasting, e.g. YouTube, Twitch, TikTok								
Mobile phones may be brought to school								
Use of mobile phones for learning at school								
Use of mobile phones in social time at school								
Taking photos on mobile phones/cameras								
Use of other personal devices, e.g. tablets, gaming devices								
Use of personal e-mail in school, or on school network/wi-fi								

Use of school e-mail for personal e-mails								

360safe
the online safety self-review tool



Designated Safeguarding Lead (DSL) notified of an Online Safety incident[1]

Carry out immediate safeguarding actions necessary to protect individuals

Unsuitable or inappropriate materials or activity

Illegal materials or activities found/suspected

Convene Safeguarding Incident Review Meeting

Investigate incident and discuss with the learner / staff / to determine what happened

Update parents/carers on incident as applicable

Ensure the wellbeing of those involved is addressed.

Ensure Incident Log is updated and make available as required

Review policies & processes and identify learning opportunities

Ensure updates to practice are shared with staff

Implement changes and monitor situation.

Wellbeing of a child potentially at risk

Staff, volunteer or other adult

Follow established safeguarding arrangements and report to the Police immediately

Refer to the LA, LADO and follow HR processes

Secure and preserve evidence in-line with Police/DOS/Safeguarding advice. Remember, do NOT investigate yourself.

Await Police response

If no illegal activity or content is confirmed, revert to internal procedures

If illegal activity or content is confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.

In the case of a member of staff or volunteer, it is possible that a suspension will take place at the point of referral to the Police whilst investigations are undertaken. Always ensure DOS advice and HR processes are correctly applied and followed

[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.

[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

Responding to Learner Actions

Incidents	Refer to class teacher/tutor	Refer to Designated Safeguarding Lead	Refer to Headteacher	Refer to Police/Childrens Services	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/ network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X	X					
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords	X								
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X					X		X	
Unauthorised downloading or uploading of files or use of file sharing.	X					X		X	
Accidentally accessing offensive or pornographic material and failing to report the incident.	X					X			
Deliberately accessing or trying to access offensive or pornographic material.		X	X			X		X	
Unauthorised use of digital devices (including taking images)	X	X	X			X		X	
Unauthorised use of online services	X	X	X			X		X	

Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X	X			X		X	

Responding to Staff Actions

Incidents	Refer to Headteacher	Refer to local authority/HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal	X	X	X				
Actions which breach data protection or network / cyber-security rules.	X	X		X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X		X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X			X
Using proxy sites or other means to subvert the school's filtering system.	X	X	X	X			X
Unauthorised downloading or uploading of files or file sharing	X						
Breaching copyright/ intellectual property or licensing regulations (including through the use of AI systems)	X	X		X			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	X	X			X		
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X			X		X

Incidents	Refer to Headteacher	Refer to local authority/HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers	X	X	X	X			X
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	X	X			X		
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X			X	X		
Actions which could compromise the staff member's professional standing	X				X		
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X					X
Failing to report incidents whether caused by deliberate or accidental actions	X						
Continued infringements of the above, following previous warnings or sanctions.	X	X					X