

Online Safety Policy

Edendork Primary School

2021-22



Review of this Policy

This online safety policy has been developed and reviewed by the school Principal and ICT Co-ordinator, in consultation with Staff and Governors.

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Board of Governors on:	
The implementation of this online safety policy will be monitored by the:	School Principal ICT Co-ordinator Safeguarding Team
Monitoring will take place at regular intervals:	Once per year
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	November 2022
Should serious online safety incidents take place, the following external persons/agencies should be informed (as appropriate):	c2k manager EA Child protection Services PSNI

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys/questionnaires of
 - pupils
 - parents/carers
 - staff

Scope of the Policy

This policy applies to all members of the Edendork Primary School community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

Edendork Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within Edendork Primary School:

Board of Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Board of Governors has taken on the role of Online Safety Governor ([it is suggested that the role may be combined with that of the Child Protection/Safeguarding Governor](#)). The role of the Online Safety Governor will include:

- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to Board of Governors

Principal and Senior Leaders

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the ICT Co-ordinator and Safeguarding team.
- The Principal and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant disciplinary procedures).
- The Principal and Senior Leaders are responsible for ensuring that the ICT Co-ordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the ICT Co-ordinator.

ICT Co-ordinator

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the relevant bodies
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- reports regularly to Senior Leadership Team/Safeguarding team

c2k

Those with technical responsibilities are responsible for ensuring:

- that Edendork Primary School's technical infrastructure is secure and is not open to misuse or malicious attack
- that Edendork Primary School meets required online safety technical requirements and any *EA* online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current *Edendork Primary School* online safety policy and practices
- they have read, understood and signed the staff acceptable use policy/agreement
- they report any suspected misuse or problem to the Principal/ICT Co-ordinator for investigation
- they have access to the *Safer Schools NI App* produced by the INEQE Safeguarding Group
- all digital communications with pupils/parents/carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices

- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- **See also EA Publication – Online Safety Advice**
<https://www.eani.org.uk/sites/default/files/2020-06/Online%20Safety%20Advice.pdf>

Designated Safeguarding Team

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

Pupils:

- **are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement**
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that Edendork Primary School's online safety policy covers their actions out of school, if related to their membership of the school

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Edendork Primary School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, school website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/Learning Platform (eg Clasdojo) and on-line pupil records
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems or programmes as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of PDMU and in line with the preventative 'Keeping Safe' education programme for primary schools devised by NSPCC
<https://learning.nspcc.org.uk/services/keeping-safe-preventative-education-in-northern-ireland>
<https://projectevolve.co.uk/>
- The planned online safety curriculum should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- *Pupils should be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.*
- *Staff should act as good role models in their use of digital technologies, the internet and mobile devices*
- *in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*
- *Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*
- *It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that C2k can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*

Education – Parents/carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Edendork Primary School will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, school web site, Classdojo
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. [swgfi.org.uk](http://www.childnet.com/parents-and-carers), www.saferinternet.org.uk/, <http://www.childnet.com/parents-and-carers>

Parents can register with the **Safer Schools NI app** for safeguarding resources and up-to-date advice on online safety.

Education – The Wider Community

Edendork Primary School will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- Providing family learning courses in use of new digital technologies, digital literacy and online safety (when appropriate)

- The school website will provide online safety information for the wider community
- Sharing their online safety expertise/good practice with other local schools

Education & Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- It is expected that some staff may identify online safety as a training need within the PRSD process.
- The ICT Co-ordinator will receive regular updates through attendance at external training events (e.g. from SWGfL/EA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The ICT Co-ordinator will provide advice/guidance/training to individuals as required.
- All teachers have access to the *Safer Schools NI App* for 'Online Safety Guidance' and 'Online Safety Help' as well as 'Daily Safeguarding Updates'.

Training – Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered as participation in school training/information sessions for staff or parents.

Technical – infrastructure/equipment, filtering and monitoring - C2k

In the C2k Acceptable Use policy (EN047) it clearly outlines that:

- C2k services are monitored
- All users are responsible for the secure use of C2k user names and passwords and appropriate use of email and the Internet
- The school has the right to access user's data and mailboxes
- Parents/carers are responsible for their children's out-of-school online use of C2k services
- Attempts to bypass filtering, or to access inappropriate or illegal material, will be reported to the school authority via C2k
- Email messages are subject to C2k's filtering policy
- Files stored within the school's network environment on servers, computers and devices will not be regarded as private and that the school reserves the right (or C2k at school's request) to monitor, review and examine the internet history, usage, communications and files of all users, and, where it deems it to be necessary, will intercept and delete material on school laptops, servers, network devices and e-mail systems, which it considers inappropriate, and prohibit the use of such material.

For details on user Network Drive Permissions see the Appendix in EN135 'Using the File & Folder Permission Tool' and EN039 for more information on 'Managing Internet Filtering'.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform (Classdojo) and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

The school acceptable use agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies

- The school allows:

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device ¹	Student owned	Staff owned	Visitor owned
Allowed in school	<i>Yes</i>	<i>Yes</i>	<i>Yes</i>	<i>Yes – with teacher permission Yes</i>	<i>Yes</i>	<i>Yes</i>
Full network access	<i>Yes</i>	<i>Yes</i>	<i>Yes</i>			
Internet only				<i>Yes</i>	<i>Yes</i>	<i>Yes</i>
No network access						

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

¹ Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation and in line with our school policy.

Communication Technologies

When using communication technologies, the school considers the following as good practice:

- The official school email service and ClassDojo may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the ICT Co-Ordinator or Safeguarding Team – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (Classdojo, email, Google Classroom, etc) must be professional in tone and content.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

Edendork Primary School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy

- Personal communications which do not refer to or impact upon the school are outside the scope of this policy

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by The Principal to ensure compliance with the school policies.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

Edendork Primary School believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	

Promotion of extremism or terrorism				X
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X
Activities that might be classed as cyber-crime under the Computer Misuse Act: <ul style="list-style-type: none"> 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
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X
Using school systems to run a private business				X
Infringing copyright				X
On-line gaming (educational)		X		
On-line gaming (non-educational)		X		
On-line gambling				X
On-line shopping/commerce		X		
File sharing		X		
Use of social media		X		
Use of messaging apps		X		
Use of video broadcasting e.g. Youtube		X		

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

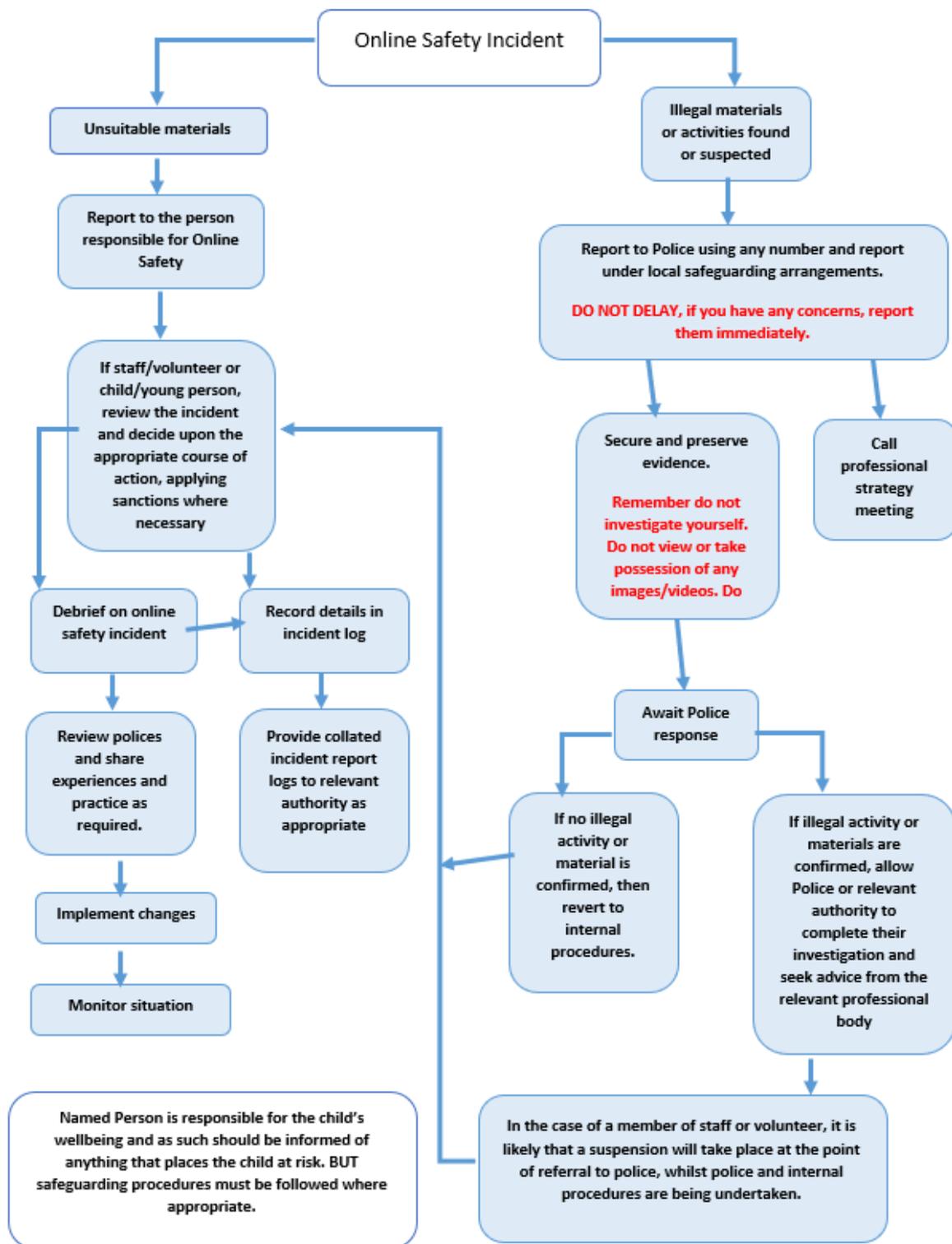
If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (page 12) for responding to online safety incidents and report immediately to the police.

School actions & sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Advice and guidance on these matters is regularly updated on the *Safer Schools App*.





Acknowledgements

This policy has been developed in line with guidance and following templates from SWGfL and C2k.

SWGfL would like to acknowledge the contribution of a wide range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of the online safety policy templates and of the 360 degree safe online safety self-review tool.

Copyright of these template policies is held by SWGfL. Schools/academies and other educational institutions are permitted free use of the Template Policies for the purposes of policy writing, review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (onlinesafety@swgfl.org.uk) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in January 2020. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.

© South West Grid for Learning Trust Ltd 2020



Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre – <https://www.saferinternet.org.uk/>

South West Grid for Learning - <https://swgfl.org.uk/products-services/online-safety/>

Childnet – <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

Revenge Porn Helpline - <https://revengepornhelpline.org.uk/>

Internet Watch Foundation - <https://www.iwf.org.uk/>

Report Harmful Content - <https://reportharmfulcontent.com/>

CEOP

CEOP - <http://ceop.police.uk/>

ThinkUKnow - <https://www.thinkuknow.co.uk/>

Others

LGfL – [Online Safety Resources](#)

Kent – [Online Safety Resources page](#)

INSAFE/Better Internet for Kids - <https://www.betterinternetforkids.eu/>

UK Council for Internet Safety (UKCIS) - <https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

Netsmartz - <http://www.netsmartz.org/>

Tools for Schools

Online Safety BOOST – <https://boost.swgfl.org.uk/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

360Data – online data protection self-review tool: www.360data.org.uk

SWGfL Test filtering - <http://testfiltering.com/>

UKCIS Digital Resilience Framework - <https://www.gov.uk/government/publications/digital-resilience-framework>

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - <http://enable.eun.org/>

SELMA – Hacking Hate - <https://selma.swgfl.co.uk>

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour -

<http://www.scotland.gov.uk/Publications/2013/03/7388>

DfE - Cyberbullying guidance -

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit:

<http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit>
[Childnet – Project deSHAME – Online Sexual Harrassment](#)
[UKSIC – Sexting Resources](#)
Anti-Bullying Network – <http://www.antibullying.net/cyberbullying1.htm>
[Ditch the Label – Online Bullying Charity](#)
[Diana Award – Anti-Bullying Campaign](#)

Social Networking

Digizen – [Social Networking](#)
UKSIC - [Safety Features on Social Networks](#)
[Children’s Commissioner, TES and Schillings – Young peoples’ rights on social media](#)

Curriculum

SWGfL Evolve - <https://projectevolve.co.uk>
[UKCCIS – Education for a connected world framework](#)
Teach Today – www.teachtoday.eu/
Insafe - [Education Resources](#)

Data Protection

[360data - free questionnaire and data protection self review tool](#)
[ICO Guides for Education \(wide range of sector specific guides\)](#)
[DfE advice on Cloud software services and the Data Protection Act](#)
[IRMS - Records Management Toolkit for Schools](#)
[NHS - Caldicott Principles \(information that must be released\)](#)
[ICO Guidance on taking photos in schools](#)
[Dotkumo - Best practice guide to using photos](#)

Professional Standards/Staff Training

[DfE – Keeping Children Safe in Education](#)
DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)
[Childnet – School Pack for Online Safety Awareness](#)
[UK Safer Internet Centre Professionals Online Safety Helpline](#)

Infrastructure/Technical Support

[UKSIC – Appropriate Filtering and Monitoring](#)
[SWGfL Safety & Security Resources](#)
Somerset - [Questions for Technical Support](#)
NCA – [Guide to the Computer Misuse Act](#)
NEN – [Advice and Guidance Notes](#)

Working with parents and carers

[Online Safety BOOST Presentations - parent’s presentation](#)
[Vodafone Digital Parents Magazine](#)
[Childnet Webpages for Parents & Carers](#)

[Get Safe Online - resources for parents](#)

[Teach Today - resources for parents workshops/education](#)

[Internet Matters](#)

Prevent

[Prevent Duty Guidance](#)

[Prevent for schools – teaching resources](#)

[NCA – Cyber Prevent](#)

Childnet – [Trust Me](#)

Research

[Ofcom –Media Literacy Research](#)

Further links can be found at the end of the UKCIS [Education for a Connected World Framework](#)



Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MAT	Multi Academy Trust
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS [Education for a Connected World Framework](#)

