CUED SPEECH UK

Makes spoken language visible for
deaf babies, children and adults

Cued Speech UK Online Safety Policies

Partners:

UK Safer Internet Centre

SW GRID for LEARNING

Funded by:

CUED SPEECH UK
Makes spoken language visible for
deaf babies, children and adults

Contents

Partners: UK Safer Internet Centre; SW Grid for Learning

Funded by:

Introduction to the Online Safety Policy

This Online Safety Policy is intended to help organisations and groups that work with children and young people to produce a suitable online safety policy which will consider all current and relevant issues and help safeguard and protect the children / young people in their care and the adults that work with them. For simplicity, the term “group” will be used throughout the document to refer to relevant organisations and groups.

The development and expansion of the use of digital technologies, and particularly of the internet, has transformed the way in which we communicate with each other. Young people, in particular, have embraced the use of these new technologies. Often, those who work with children and young people find it difficult to keep up to date with these changes and the impact that they can have on their lives.

What do we mean by “online”?

When we refer to being online we include being connected to a wide range of devices or technologies, such as computers, the internet, mobile phones, hand held devices, games consoles and many more.

Why do you need online safety policies?

An online safety policy:

- Sets clear expectations for how technology should be used.
- Provides a single point of information and raises awareness for staff and volunteers.
- Helps to protect the group and its members in the event of an adverse incident or challenge
- Forms part of the group’s protection from legal challenge, relating to the use of these new technologies
- Provides clear guidance for managing risk, whilst making the most of opportunities that new technologies offer.

Are you part of a wider organisation or association?

Many groups that work with young people will be part of wider national or local organisations – whether statutory or voluntary. In this case, you should check if they already have relevant policies and guidance that should be taken into account when developing your policy.

CUED SPEECH UK

Makes spoken language visible for
deaf babies, children and adults

CUED SPEECH UK

Online Safety Policy

CUED SPEECH UK

Partners:

Funded by:

CUED SPEECH UK
Makes spoken language visible for
deaf babies, children and adults

Online Safety Policy

Background / Rationale

Partners: UK Safer Internet Centre; SWGfL (South West Grid for Learning)

Funded by:

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work with children and young people are bound.

Digital technologies have become integral to the lives of children and young people in today's society. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Children / young people, staff and volunteers have a right to safer internet access at all times.

However, the use of these new technologies can put users at risk. Some of the dangers may include:

- Access to illegal, harmful or inappropriate images or other content
- Loss of privacy / control of personal information
- Grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- Hacking, viruses and system security
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other policies (eg safeguarding / child protection policies).

As with all other risks, it is impossible to eliminate the risks completely. By providing good examples / role models and by raising awareness, it is possible to build the resilience of children and young people, so that they have the confidence and skills to deal with these risks.

We have provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The online safety policy that follows explains how we intend to do this.

Development / Monitoring / Review of this Policy

This online safety policy was developed by	Cued Speech Executive Director Henrietta Ireland
These people were consulted in the development of the policy	• John Woodhouse Director of 'Dialogue' external safeguarding consultants • Henrietta Ireland Executive Director • Louise Creed Cued Speech Office Manager • Cate Calder Training Lead Cued Speech • Kathy Kenny Lead Cued Speech Regional Adviser • Chrissie Hardy Chair of Trustees Cued Speech • Volunteers • Parents and Carers
This online safety policy was approved by	Cued Speech UK Board of Trustees James Bird Children in Need
On	*05/08/21*
The implementation of this online safety policy will be monitored by the:	John Woodhouse 'Dialogue' Safeguarding Consultants
Monitoring will take place at regular intervals:	Annually
Monitoring reports will be presented to:	*Henrietta Ireland* *Chrissie Hardy* *John Woodhouse*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new development. The next anticipated review date will be:	*Aug 2022*
Should serious online incidents take place, the following external persons / agencies should be informed:	• **Local Authority Child Protection Lead Person**

	• **Local Authority Designated Officer (LADO) (if it involves an allegation against member of staff / volunteer)** • **Police**

Scope of the Policy

This policy applies to all members of the group (including staff, volunteers, children and young people, parents / carers, visitors, community users) who have access to and are users of communications technologies (whether these belong to the group or to the users themselves)

Roles and Responsibilities

The following section outlines the roles and responsibilities for the online safety of users within the group.

National Charity: Number

- Our National Charity, Cued Speech UK has relevant online safety / safeguarding policies and guidance. Staff, volunteers and all users should be aware of these guidelines which are
    - available from Henrietta Ireland ED, Louise Creed Business Manager and Debbie Hawke Admin Lead
    - included / referred to in this policy document
- Staff, volunteers and users are also governed by relevant legislation, which is referred to in this policy and by the guidance provided by the Local Safeguarding Children's Board (with regard to safeguarding / child protection and how incidents should be reported)..

Group Leader:

- The Leader, Henrietta Ireland, has overall responsibility for ensuring the safety (including online safety) of all staff, volunteers and members of the group, though the day to day responsibility for online safety may be delegated to Louise Creed or Debbie Hawke.
- Both Henrietta Ireland and Louise Creed are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff or volunteer. (see flow chart on dealing with online safety incidents – included in a later section)
- Henrietta Ireland is responsible for ensuring that the Online Safety Lead Person and other relevant staff / volunteers receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant
- Henrietta Ireland will ensure that there is a system in place to allow for the monitoring of online safety in the Charity and that they receive regular monitoring reports.

CUED SPEECH UK

Makes spoken language visible for
deaf babies, children and adults

Partners:

Funded by:

Online Safety Lead Person:

The Online Safety Lead Person: Henrietta Ireland Executive Director Cued Speech UK

- **ensures that staff / volunteers have an up to date awareness of the group's current online safety policy and practices**
- **ensures that all staff / volunteers are aware of the procedures that need to be followed in the event of an online safety incident taking place.**
- **takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the online safety policies / documents**
- **offers advice and support for all users**
- **keeps up to date with developments in online safety**
- **understands and knows where to obtain additional support and where to report issues**
- **ensures provision of training and advice for staff and volunteers**
- **liaises with the national / local organisation / association as relevant**
- **receives reports of online safety incidents and creates a log of incidents to inform future online safety developments, communicates with parents and carers**
- **monitors incident logs**
- **leads the online safety group**

The Lead Person should be trained in online safety issues and be aware of the potential for serious child protection issues.

Staff and volunteers

are responsible for ensuring that:

- they have an up to date awareness of the group's current online safety policy and practices
- they have read, understood and signed the Staff / Volunteer Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the relevant person (insert title) – particularly where it is believed that a child's welfare is at risk.
- digital communications with children and young people should be on a professional level and where possible only carried out using the official systems of the group.

- they are aware of online safety issues particularly those related to the use of mobile phones, cameras, gaming consoles and hand held devices and that they monitor their use and implement the group policies with regard to these devices

Children and young people:

- are expected to abide by the Acceptable Use Policy / Rules, which they may be expected to sign (depending on their age) before being given access to the organisation’s systems and devices
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should demonstrate positive online behaviour

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.
Parents / carers should sign the relevant permission forms on the taking and use of digital and video images.

Policy Statements

Educating children and young people to stay safe online

Whilst regulation and technical solutions are very important, their use should be balanced by making children and young people aware of the need to take a responsible approach to online safety. Children and young people need help and support to recognise and avoid online safety risks and build their resilience. Online safety awareness will be provided in the following ways:

- **Key online safety messages should be reinforced as part of all relevant planned programmes of activities for young people.**
- **Online safety issues should be discussed / highlighted, when possible, in informal conversations with young people.**
- **When the opportunity arises young people should be advised to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information**

Awareness raising for parents / carers

We should provide online safety information and awareness to parents and carers through:

- **Letters, newsletters, web site.**
- **Meetings with parents / carers (formal and informal).**

- **Reference to the SWGfL (South West Grid for Learning) Safe website (nb the SWGfL “Golden Rules” for parents) and other relevant resources.**
- **sharing the group’s policies with parents and carers.**
- **Providing leaflets and inforamation around staying safe on line NSPCC and O2 information for parents**

Training – staff and volunteers

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

- **A planned programme of training about online safety will be made available to staff and volunteers.**
- **All new staff and volunteers will receive awareness training as part of their induction programme, ensuring that they fully understand the online safety policy and acceptable use policies**
- **An audit of the online safety training needs of all staff will be carried out regularly**
- **The online safety Lead Person (or other nominated person) will receive regular updates through attendance at relevant external training events and / or by reviewing guidance documents released by the national organisation / SWGfL / the local authority and others.**
- **This online safety policy and its updates will be presented to and discussed by staff and volunteers at staff / team meetings.**

Protecting the professional identity of staff and volunteers

This applies to any adult, but particularly those working with children and young people (paid or unpaid) within the group. Consideration should be given to how your online behaviour may affect your own safety and reputation and that of the group.

Communication between adults and between children / young people and adults, by whatever method, should take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, e-mails, digital cameras, videos, web-cams, websites and blogs.

When using digital communications, staff and volunteers should:

- **only make contact with children and young people for professional reasons and in accordance with the policies and professional guidance of the group**
- **not share any personal information with a child or young person eg should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers.**
- **not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.**
- **be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.**
- **ensure that all communications are transparent and open to scrutiny.**
- **be careful in their communications with children so as to avoid any possible misinterpretation.**
- **ensure that if they have a personal social networking profile, details are not shared with children and young people or parents (making every effort to keep personal and professional online lives separate).**
- **not post information online that could bring the group into disrepute.**
- **be aware of the sanctions that may be applied for breaches of policy related to professional conduct.**
- ***E-mail, text or other web based communications between staff / volunteers and a child / young person should (wherever possible) take place using the group's official equipment / systems.***
- ***Any communications outside the agreed protocols (above) may lead to disciplinary and/or criminal investigations.***

Wider personal use of digital communications:

While the section above refers to communications between staff / volunteers and children / young people consideration should also be given to how the use of digital communications by staff and volunteers in their private lives could have an impact on the reputation of themselves and the group. Everyone should be able to enjoy the benefits of digital technologies. Staff and volunteers should, wherever possible, seek to separate their professional online presence from their online social life and take the following into account when using these digital communications:

- Careful consideration should be given as to who should be included as "friends" on social networking profiles and which information / photos are available to those friends
- Privacy settings should be frequently reviewed.
- The amount of personal information visible to those on "friends" lists should be carefully managed and users should be aware that "friends" may still reveal or share this information
- "Digital footprint" – information, including images, posted on the web may remain there for ever. Many people subsequently regret posting information that has become embarrassing or harmful to them

- A large proportion of employers engage in searches of the internet when selecting candidates and are influenced by the content they find.

Your technology

The group will be responsible for ensuring that all systems and devices will be as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Systems and devices will be managed in ways that ensure that the group meets accepted online safety requirements, as below:

Systems and devices will be regularly monitored and users are made aware of this in the Acceptable Use Policy.

- **Personal data must not be sent over the internet or taken away from the group's offices / facilities unless safely encrypted or otherwise secured.**
- **The systems and devices needing protection will be identified. These could be: computers; any device with internet access; networks (hard wired or wireless**
- **Devices in use are protected against online security threats, such as: viruses; unauthorised access; spyware and malware.**
- **Passwords will be provided, where required, for those who need access to these systems / devices and access will be restricted for those who do not. Users will be required to change their password regularly. Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.**
- **The "master / administrator" passwords for the systems / devices must be available to Henrietta Ireland or Louise Creed and kept in a secure place (eg a safe).**
- **Changes to systems and devices can only be made by those who have permission to do so eg installing software or changing security systems**

How you use technology to communication

When using communication technologies the group considers the following as good practice:

- **The group's official email service may be regarded as safe and secure and is monitored. Staff and volunteers should therefore use only the group's email service, where available, to communicate with others when that communication is related to the group.**
- **Users must immediately report, to a nominated person, Henrietta Ireland or Louise Creed – in accordance with the group's policy, the receipt of any communication that**

makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such communication.

- **Any communication between staff / volunteers and the children / young people or their parents / carers must be professional in tone and content. These communications should, where possible, only take place on official (monitored) systems.**
- **Personal information should not be posted on the group website and, where possible, only official email addresses should be used to identify members of staff.**

Use of digital and video images

The development of digital imaging technologies has created significant benefits, allowing users instant use of images that they have recorded themselves or downloaded from the internet. However, staff / volunteers and children / young people need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The group will raise awareness about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **When using digital images, staff and volunteers should raise awareness among children / young people and their parents about the risks associated with the taking, use, sharing, publication and distribution of images**
- **Written permission from parents or carers will be obtained to allow images to be taken of their children / young people and also allowing their use for legitimate activities or for publicity that reasonably celebrates success and promotes the work of the group.**
- **Parents / carers are allowed to take digital / video images of their children at group special events within the guidelines contained in the Parents / Carers Template Permission Form in the Supporting Policies.**
- **Staff and volunteers are allowed to take digital / video images, where appropriate, but must follow the group policies concerning the sharing, distribution and publication of those images. Those images should be taken, where possible, on the organisation's equipment, not the personal equipment of staff and volunteers.**
- **Care should be taken when taking digital / video images that young people are appropriately dressed and are not participating in activities that might bring the individuals or the group into disrepute.**
- **If photos are taken, their storage and use must not cause risk or embarrassment.**
- **Photographs published on the website, or elsewhere that include young people will be selected carefully and will comply with good practice guidance on the use of such images.**
- **The full names of young people will not be used anywhere on a website, blog, or published article, particularly in association with photographs. Consideration should be given to media coverage and journalists should be made aware of this policy.**

Data Security

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Only transferred to others with adequate protection.

Staff and volunteers must ensure that they:
At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer personal data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
  - the data should be encrypted and password protected
  - the device should be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
  - *the device should offer approved virus and malware checking software*
  - *the data should be securely deleted from the device, once it has been transferred or its use is complete*

Unsuitable / inappropriate activities

The group believes that the activities referred to in the following section would be inappropriate in a context of working with young people. The group policy restricts certain internet usage as follows:

User Actions

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**					√
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					√
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					√
	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					√
	pornography				√	
	promotion of any kind of discrimination				√	
	threatening behaviour, including promotion of physical violence or mental harm				√	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the group or brings the group into disrepute				√	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards that are in place					√	
Infringing copyright					√	
Revealing or publicising confidential information (eg financial / personal information, computer / network access codes and passwords)					√	
Creating or propagating computer viruses or other harmful files					√	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					√	
Using the group systems to run a private business						

On-line gaming (educational)					
On-line gaming (non educational)					
On-line gambling					
On-line shopping / commerce					
File sharing (eg Bit Torrent, Limewire)					
Use of personal social networking sites(while "at work")					
Use of an official group social networking site					
Use of video broadcasting eg Youtube					

Sanctions Chart

The group needs to have clear and manageable procedures when dealing with misuse. It is more likely that the organisation will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and proportionately and are recorded and well communicated.

If staff / volunteers suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the “Procedure for Reviewing Internet Sites for Suspected Harassment and Distress” should be followed. This guidance recommends that more than one member of staff / volunteer is involved in the investigation which should be carried out on a “clean” designated computer.

It is intended that incidents of misuse will be dealt with through any accepted disciplinary procedures as follows:

Young People

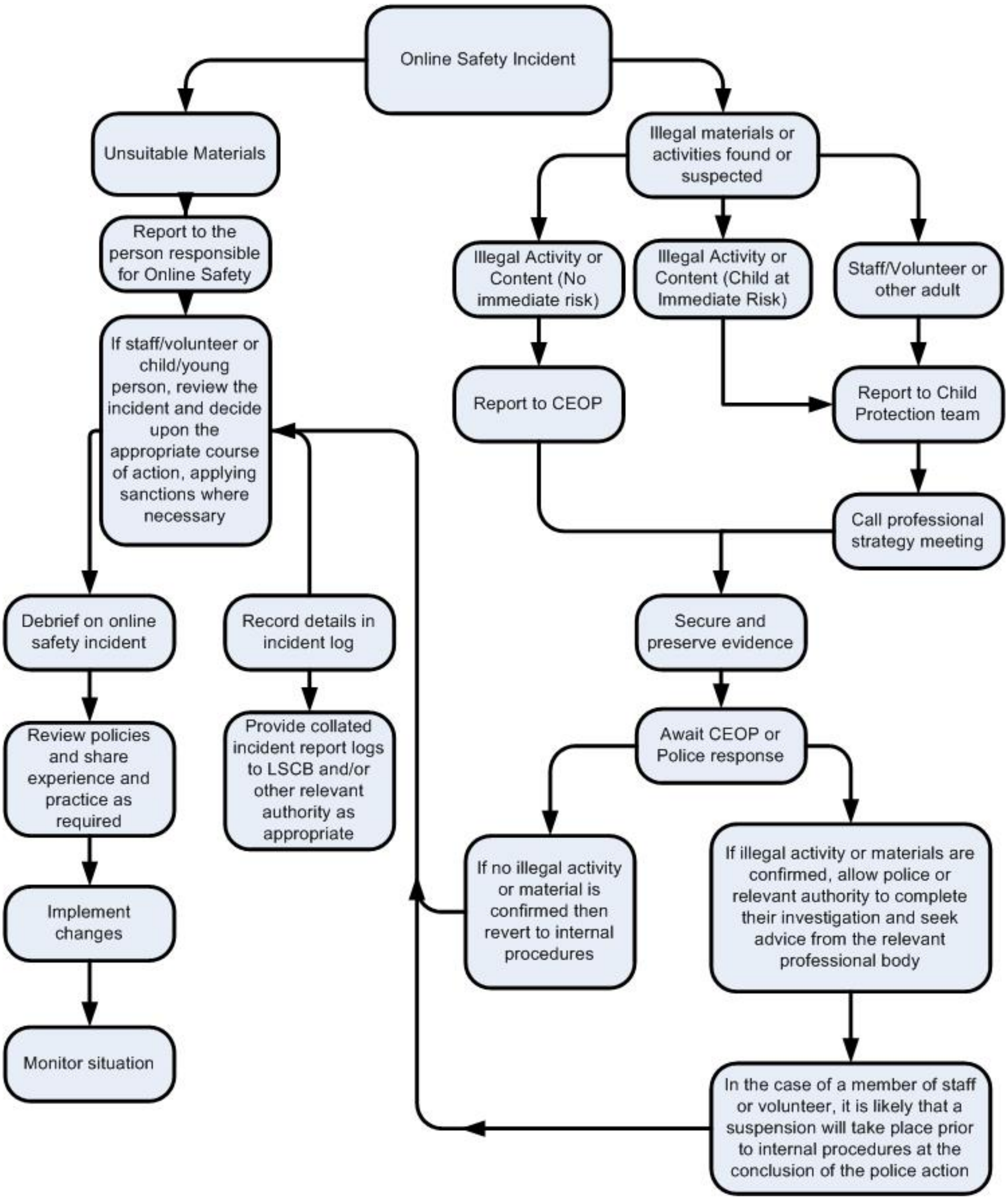
Incidents:	Refer to Leader	Refer to Police	Requires technical response / support	Inform parents / carers	Removal of access to technology / devices	Warning	*Further sanction (to be described)*
Accessing or trying to access illegal material (see list in earlier section on unsuitable / inappropriate activities).	√	√		√			
Unauthorised downloading or uploading							
Allowing others to access technology / devices by sharing username and passwords							
Attempting to access or accessing the technology / devices, using another person's account (hacking)							
Corrupting or destroying the data of other users							
Sending a communication that is regarded as offensive, harassment or of a bullying nature							
Actions which could bring the organisation into disrepute.							
Deliberately accessing materials that the group has agreed is inappropriate							
Activities that infringe copyright or data protection.							
Using proxy by-pass sites or other means to subvert the filtering system							
Accidentally accessing materials that the group has agreed is inappropriate and failing to report it.							
Unauthorised use of mobile phone / digital camera / other handheld device							
Unauthorised use of social networking / instant messaging / personal email							

Staff and volunteers

Incidents:	Refer to line manager / Leader	Refer to National / Local Organisation / body	Refer to Police	Requires technical response / support	Warning	Suspension	Disciplinary action
Accessing or trying to access illegal material (see list in earlier section on unsuitable / inappropriate activities).	√	√	√				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email "while at work"							
Unauthorised downloading or uploading of files							
Disclosing passwords or any information relating to the security of technology and devices.							
Accidental infringement of the organisation's personal data policy							
Deliberate infringement of the organisation's personal data policy							
Corrupting or destroying the data of other users							
Deliberate damage to hardware or software							
Sending a communication that is offensive, harassment or of a bullying nature							
Using personal communication technologies eg email / social networking / instant messaging / text messaging to communicate with young people (except where allowed in the policy)							
Actions which could compromise the professional integrity of staff / volunteers							

Bringing the organisation into disrepute							
Deliberately accessing materials that the group has agreed is inappropriate							
Breaching copyright or licensing regulations							
Using proxy by-pass sites or other means to subvert the filtering system							
Accidentally accessing materials that the group has agreed is inappropriate and failing to report it.							

Flowchart for responding to online safety incidents


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are 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 likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Supporting Policies

Partners:

UK Safer Internet Centre

SWGfL GRID for LEARNING

Funded by:

CUED SPEECH UK

Makes spoken language visible for
deaf babies, children and adults

On the following pages you will find a range of supporting policies:

Management:

1. Template acceptable use policy for children and young people (older children)
2. Template acceptable use policy for young children (eg age 8 or younger)
3. Template accptable use policy for staff and volunteers (including professional identity)
4. Template consent form for parents and carers (including use of images)
5. Template personal data policy

People:

1. Flowchart for responding to online safety incidents
2. Guidance for reviewing internet sites (for suspected harassment and distress)
3. Template reporting log
4. Template training needs audit

Technology

1. Template password security policy
2. Template monitoring log

At the end of this document you will find:

Links to other organisations and documents

Legislation

Glossary

Acknowledgements

Partners:

Funded by:

CUED SPEECH UK
Makes spoken language visible for
deaf babies, children and adults

Supporting Policy M1

Acceptable Use Policy Agreement

I understand that while I am a member of Cued Speech UK. I must use technology in a responsible way.

For my own personal safety:

- I understand that my use of technology will be supervised and monitored.
- I will keep my password safe and will not use anyone else's (even with their permission)
- I will keep my own personal information safe as well as that of others.
- I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

For the safety of others

I will not interfere with the way that others use their technology.

- I will be polite and responsible when I communicate with others,
- I will not take or share images of anyone without their permission.

For the safety of the group:

- I will not try to access anything illegal
- I will not download anything that I do not have the right to use.
- I will only use my personal device if I have permission and use it within the agreed rules
- I will not deliberately bypass any systems designed to keep the group safer.
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes of any type on the devices belonging to the group, without permission.
- I will only use social networking,and chat sites with permission I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines:

Name

Signature

Date

The group could choose to:

- Use this AUP as a signed agreement
- Provide copies to each user as guidance
- Include it within a handbook or induction materials
- Display as a poster or separate statement wherever technology is used

Partners:

UK Safer Internet Centre

SW GRID for LEARNING

Funded by:

Template Policies –
Acceptable Use Agreement for Staff and Volunteers

Background

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure that:

- Staff and volunteers will act responsibly to stay safer while online, being a good role model for younger users.
- effective systems are in place for the online safety of all users and the security of devices, systems, images, personal devices and data.
- staff and volunteers are aware of and can protect themselves from potential risk in their use of online technologies.

The term “professional” is used to describe the role of any member of staff, volunteer or responsible adult.

For my professional and personal safety I understand that:

- I will ensure that my on-line activity does not compromise my professional responsibilities, nor bring my group into disrepute.
- My use of technology could be monitored.
- When communicating professionally I will use the technology provided by the group (eg email
- These rules also apply when using the group’s technology either at home or away from the group base.

For the safety of others:

- **I will not access, copy, remove or otherwise alter any other user’s files, without authorisation.**
- **I will communicate with others in a professional manner.**
- **I will share other’s personal data only with their permission.**
- **I understand that any images I publish will be with the owner’s permission and follow the group’s code of practice.**
- **Wherever possible I will use the group’s equipment to record any digital and video images, unless I have permission to do otherwise.**

CUED SPEECH UK
Makes spoken language visible for
deaf babies, children and adults

For the safety of the group, I understand that:

- **I will not try to access anything illegal, harmful or inappropriate. It is my responsibility to immediately report any illegal, harmful or inappropriate incident.**
- **I will not share my online personal information (eg social networking profiles) with the children and young people in my care. I will not deliberately bypass any systems designed to keep the group safer.**
- **I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Personal Data Policy** (or other relevant policy). **Where personal data is transferred, externally, it must be encrypted.**
- **I understand that data protection policy requires that any personal data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by the organisation's / group's policy to disclose such information to an appropriate authority.**
- **Personal passwords and those of other users should always be confidential.**
- **I will not download anything that I do not have the right to use.**
- **I will only use my personal device if I have permission and use it within the agreed rules**
- **I will inform the appropriate person if I find any damage or faults with technology.**
- **I will not attempt to install programmes of any type on the devices belonging to the group, without permission**

Staff / Volunteer Name

Signed

Date

Partners: UK Safer Internet Centre; SW Grid for Learning

Funded by:

CUED SPEECH UK
Makes spoken language visible for
deaf babies, children and adults

Supporting Policy M4

Consent Form for Parents and Carers

A copy of the Children / Young People Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the organisation's / group's expectations of the young people in their care.

Parent / Carers Name:

Name of Child / Young person:

As the parent / carer, I give permission for my child to use the group's technology and devices.

I know that my child *has signed an Acceptable Use Agreement and* has received guidance to help them understand the importance of online safety.

I understand that the group will take reasonable precautions to ensure that my child will be safer when online, however, I understand that this manages risk but cannot eliminate it.

I understand that my child's online activity will be supervised and monitored and that the group will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I understand that the group will take appropriate action in the event of any incidents.

I will encourage my child to adopt safe use of the internet and digital technologies.

Signed **Date**

Partners: UK Safer Internet Centre SW GRID for LEARNING

Funded by:

CUED SPEECH UK
Makes spoken language visible for
deaf babies, children and adults

Use of Digital / Video Images

The use of digital / video images plays an important part in our activities. Children / young people, staff and volunteers may use digital cameras or other devices to record evidence of those activities. These images may then be used in Learning Journeys and presentations and may also be used to celebrate success through their publication in newsletters, on the website and occasionally in the public media.

The group will comply with the Data Protection Act and request parents / carers permission before taking images of their children. We will also ensure that, wherever possible, full names will not be published alongside images.

It's a great thing to film your child at our events and we know they provide a lot of precious memories. You can support us in keeping our children safe by considering the following:

- *Images and video should be for your own or family's personal use only*
- *Think about privacy and who has the right to see your images, not only of your own child but of others*
- *If you do share the images online, then you must make sure they are limited to immediate family only and not public*
- *If you need help in knowing how to do this then come and have a chat with us*

Parents / carers are requested to sign the permission form below to allow the group to take and use images of their children.

Permission Form

Parent / Carers Name ☐

Name of Child / Young Person ☐

As the parent / carer of the above child, I agree to the group taking and using digital / video images of my child / children. I understand that the images will only be used to support legitimate activities or in publicity that reasonably celebrates success and promotes the work of the group.

I agree that if I take digital or video images at group events which include images of children, other than my own, I will abide by these guidelines in my use of the images.

Signed ☐ **Date** ☐

Partners:

UK Safer Internet Centre

SW GRID for LEARNING

Supporting Policy M5

Personal Data Policy

Introduction

Personal Data

The group and individuals may have access to a wide range of personal information and data, held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about children / young people, members of staff / volunteers and parents and carers eg. names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Professional records eg. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families

It is the responsibility of all staff and volunteers to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not have permission to access that data or does not need to have access to that data. Anyone who has access to personal data must know, understand and adhere to this policy.

The Data Protection Act (1998) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow “good information handling principles”.

Guidance for organisations on the DPA is available on the Information Commissioners Office website: http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

Policy Statements

The group will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed.

Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

Responsibilities

The group leader will keep up to date with current legislation and guidance and will carry out risk assessments (as necessary).

Training & awareness

Staff and volunteers will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Meetings / briefings / training for staff / volunteers
- Day to day support and guidance from the Group Leader.

Risk Assessments

Information risk assessments will be carried out by staff / volunteers to establish key areas of the group where data might be at risk and how the risk could be reduced

Storing personal data

Personal data must be held securely on the group's premises and only accessed by those with permission to do so. Any personal data removed from the premises should have the appropriate level of protection to prevent loss of data.

Disposal of data

The group will comply with the requirements for the safe destruction of personal data when it is no longer required. Such data must be destroyed, rather than deleted and be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, and other (paper based) media must be shredded, incinerated or otherwise disintegrated.

CUED SPEECH UK

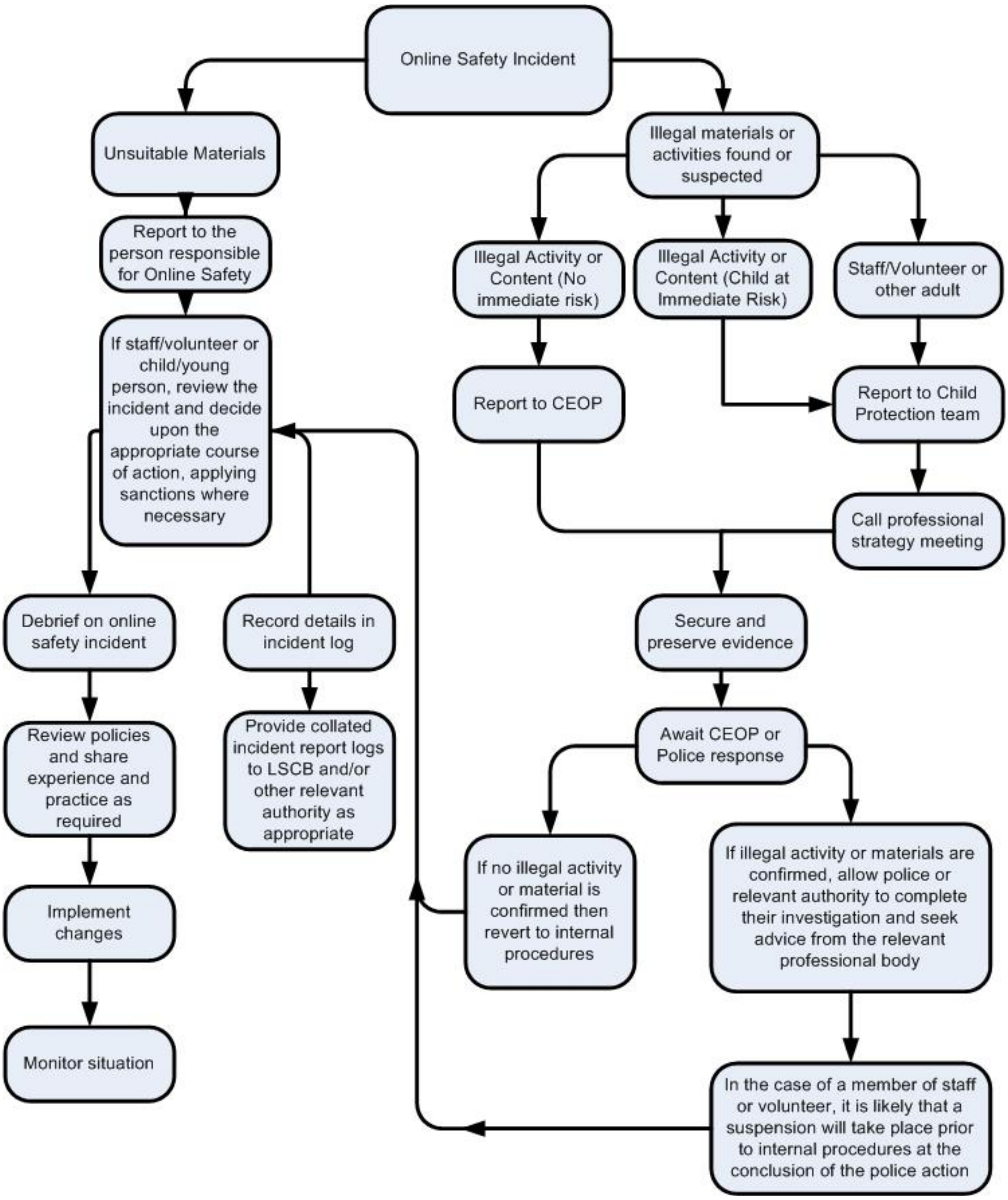
Makes spoken language visible for
deaf babies, children and adults

Supporting Policy P1

Flowchart for responding to online safety incidents

Partners:

Funded by:


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are 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 likely that a suspension will take place prior to internal procedures at the conclusion of the police action

CUED SPEECH UK

Makes spoken language visible for
deaf babies, children and adults

Supporting Policy P3

Reporting Log

Reporting Log Group……………………………

Time	Incident	Action taken		Incident Reported by	Signature
		What?	By whom?		

Partners:

Funded by:

CUED SPEECH UK
Makes spoken language visible for
deaf babies, children and adults

Supporting Policy P4

Training Needs Audit

Training Needs Audit Log Group .... Date					
Relevant training in last 12 months	Identified training need	To be met by:	Cost	Review date	Date

Partners:

Funded by:

	Position								
	Name								

Supporting Policy T1

t

Policy Statements

All users will be provided with a username and password by Louise Creed who will keep an up to date record of users and their usernames. The following rules apply to the use of passwords:

- **the “master / administrator” passwords for the group should be held by more than one person (including the senior leader), should not be used for day to day use and must be stored securely.**

Supporting Policy T2

Monitoring Log

Monitoring Log Group ……………………………	Signed								

Date	Programme / Services Monitored	Monitored by	Issues identified	Reported to

Links to other organisations or documents

The following sites will be useful as general reference sites, many providing good links to other sites:

South West Grid for Learning: (SWGfL Safe) - http://www.swgfl.org.uk/safe

Childnet - http://www.childnet.com

CEOP - Think U Know - http://www.thinkuknow.co.uk/

Netsmartz http://www.netsmartz.org/index.aspx

Teach Today http://www.teachtoday.eu/

Internet Watch Foundation – report criminal content: http://www.iwf.org.uk/

UK Council for Child Internet Safety: http://www.education.gov.uk/ukccis

Safer Internet Centre: http://www.saferinternet.org.uk/

Management

SWGfL Online Safety Planner. – for groups that work with children and young people – this self review tool allows groups that work with children to assess their policy and provision. http://www.swgfl.org.uk/ospoffline

SWGfL School e-safety policy templates: http://www.swgfl.org.uk/Staying-Safe/Content/News-Articles/Creating-an-e-safety-policy--Where-do-you-start-

Plymouth Early Years E-Safety Toolkit:
http://www.plymouth.gov.uk/early_years_toolkit.pdf

Byron Review ("Safer Children in a Digital World")
http://webarchive.nationalarchives.gov.uk/tna/+/dcsf.gov.uk/byronreview/

Guidance for safer working practice for adults that work with children and young people - http://webarchive.nationalarchives.gov.uk/20100202100434/dcsf.gov.uk/everychildmatters/resources-and-practice/ig00311/

The Learning Trust Example Online Safety Policy (Schools):
http://trustnet.learningtrust.co.uk/Trust/forms/ICT/ICT%20Policies/Internet%20Safety%20Policy.pdf

Belfast Computer Clubhouse Example:
http://www.belfastclubhouse.org/word/Membership-Form.doc

Tech Mission Safe Families AUP: http://www.safefamilies.org/aup.php

Policies for voluntary groups eg Woodcraft Folk:
http://www.woodcraft.org.uk/safeguarding

Somerset e-sense progression (e-safety curriculum:- https://slp.somerset.gov.uk/cypd/elim/somersetict/Site%20Pages/Progressions%20-%20eSense.aspx

Ofsted survey: http://www.ofsted.gov.uk/Ofsted-home/Publications-and-research/Browse-all-by/Documents-by-type/Thematic-reports/The-safe-use-of-new-technologies/(language)/eng-GB

Protecting your personal information online: http://www.ico.gov.uk/~/media/documents/library/data_protection/practical_application/protecting_your_personal_information_online.ashx

Getnetwise privacy guidance: http://privacy.getnetwise.org/

People

CBBC – stay safe: http://www.bbc.co.uk/cbbc/help/home/

Oldham LSCB Youth Council Charter of Young Peoples Digital Rights: http://www.esafetyweek.info/

NSPCC: http://www.nspcc.org.uk/help-and-advice/for-parents-and-carers/internet-safety/internet-safety_wdh72864.html

Vodafone Parents Guide: http://parents.vodafone.com/

Google guidance for parents: http://www.teachparentstech.org/

E-Parenting tutorials: http://media-wareness.ca/english/parents/internet/eparenting.cfm

Training - SWGfL EPICT: http://swgfl.org.uk/Staying-Safe/Epict/Epict

Training - SQA Internet Safety qualification: http://www.sqa.org.uk/sqa/34591.html

Practical Participation – Tim Davies: http://www.practicalparticipation.co.uk/yes/

Protecting Professional Identity documents: http://public.merlin.swgfl.org.uk/establishments/879/PlymouthChildrensServicesICTAdvice/Pages/ProtectingYourProfessionalIdentity.aspx

SWGfL Facebook guidance –

http://www.swgfl.org.uk/Staying-safe/Files/Documents/facebook-6

Digital Citizenship: http://www.digizen.org.uk/

Kent “Safer Practice with Technology”:
http://kentrustweb.org.uk/CS/community/kent_teachers/archive/2009/07/07/safer-practice-with-technology-for-school-staff.aspx

Connect Safely Parents Guide to Facebook:
http://www.connectsafely.org/Safety-Advice-Articles/facebook-for-parents.html

Ofcom – Help your children to manage the media:
http://consumers.ofcom.org.uk/2010/10/parental-controls-help-your-children-manage-their-media/

Mobile broadband guidance: http://www.mobile-broadband.org.uk/guides/complete-resource-of-internet-safety-for-kids/

Orange Parents Guide to the Internet:
http://www.orange.co.uk/communicate/safety/10948.htm

O2 Parents Guide: http://www.o2.co.uk/parents

FOSI – Family Online Internet Safety Contract: http://www.fosi.org/resources/257-fosi-safety-contract.html

Office for Internet Safety (Ireland) – guide for parents:
http://www.internetsafety.ie/website/ois/oisweb.nsf/page/safety-guideparents-en

Cybermentors (Beat Bullying): http://www.cybermentors.org.uk/

Teachernet Cyberbullying guidance:
http://www.digizen.org/resources/cyberbullying/overview

“Safe to Learn – embedding anti-bullying work in schools”
http://www.anti-bullyingalliance.org.uk/tackling_bullying_behaviour/in_schools/law,_policy_and_guidance/safe_to_learn.aspx

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm

Cyberbullying.org - http://www.cyberbullying.org/

Technology

Kaspersky – advice on keeping children safe - http://www.kaspersky.co.uk/keeping_children_safe

Kaspersky - password advice: www.kaspersky.co.uk/passwords

CEOP Report abuse button: http://www.ceop.police.uk/Safer-By-Design/Report-abuse/

Information Commissioners Office guidance on use of photos in schools: http://www.ico.gov.uk/youth/sitecore/content/Home/for_the_public/topic_specific_guides/schools/photos.aspx

Which Parental control guidance: http://www.which.co.uk/baby-and-child/child-safety-at-home/guides/parental-control-software/

How to encrypt files: http://www.dummies.com/how-to/content/how-to-encrypt-important-files-or-folders-on-your-.html

Get safe on line – Beginners Guide - http://www.getsafeonline.org/nqcontent.cfm?a_name=beginners_1

Childnet Parents and Teachers on downloading / music, film, TV and the internet - http://www.childnet.com/downloading/

Microsoft Family safety software: http://windows.microsoft.com/en-US/windows-vista/Protecting-your-kids-with-Family-Safety

Norton Online Family: https://onlinefamily.norton.com/

Forensic Software http://www.forensicsoftware.co.uk/education/clients.aspx

Legislation

Groups should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online. It is recommended that legal advice is sought in the event of an online issue or situation.

Computer Misuse Act 1990:

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject’s rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the context of work with young people, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly

Partners: Funded by:

UK Safer Internet Centre
SW GRID for LEARNING

- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers school Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
Becta	British Educational Communications and Technology Agency (Ceased to exist in March 2011, though resources are available from National Archives website)
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
DfE	Department for Education
ECM	Every Child Matters
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
Learning	A learning platform brings together hardware, software and supporting services

Platform to support teaching, learning, management and administration.

LSCB Local Safeguarding Children Board

NEN National Education Network – works with the Regional Broadband Consortia (eg SWGfL) to provide the safe broadband provision to schools across Britain.

Ofcom Office of Communications (Independent communications sector regulator)

Ofsted Office for Standards in Education, Children's Services and Skills

RBC Regional Broadband Consortia (eg SWGfL) have been established to procure broadband connectivity for schools in England. There are 10 RBCs covering 139 of the 150 local authorities:

SIC Safer Internet Centre – a partnership of SWGfL, Childnet and the Internet Watch Foundation which receives European Commission funding to organise Safer Internet Day **(SID)** each February and promote safer internet activities.

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 e-safety programmes for schools, young people and parents.

VLE Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting)

WAP Wireless Application Protocol

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this Online Safety Planner Policy Template:

- Members of the SWGfL E-Safety Group and the 360 degree safe OSP Planning Group
- Avon and Somerset Police
- Devon and Cornwall Police
- Somerset County Council
- Plymouth City Council
- North Somerset Council

Partners:

UK Safer Internet Centre

SW GRID for LEARNING

Funded by:

CUED SPEECH UK
Makes spoken language visible for
deaf babies, children and adults

- Gloucestershire County Council
- South Gloucestershire SCB
- University of Plymouth
- DfE
- Becta
- Byron Review – Children and New Technology – “Safer Children in a Digital World”

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in February 2011. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.

Partners: UK Safer Internet Centre; SW Grid for Learning

Funded by: