National Deaf Children's Society

E-Safety Policy
(Safer Working Practice with Technology)

ndcs
○ ● ○
every deaf child

Policy Summary

Document Title	E-Safety (Safer Working Practice with Technology)
Owner/s:	Peter Weston
Author/s	Annie Dodd / Peter Weston
Issuing Team/Dept.	CYPF
This Version:	1.0
Approved Version Number:	1.0
Date Approved:	7 January 2014
Review Frequency:	Full review every 3 years, annual interim checks to identify amendments required due to changes in external legislation.
Next Review Date:	January 2017
Sensitivity	Open
Circulation	Public (via website) All Staff (via Intranet) Executive Director Team / Trustees / Local Groups
Executive Director Lead:	Helen Cable

E-Safety (Safer Working Practice with Technology)

INDEX

		Page
1	Introduction	3
2	Policy Statement	4
3	Areas of Concern	5
4	Protecting Staff and Volunteers	6
5	Responsibilities of All Technology Users	6
6	Responsibilities of Senior Management	7
7	Key Responsibilities of Designated Manager and Designated Persons	8
8	Key Responsibilities of IT Teams	8
9	Key Responsibilities of NDCS Managers, Staff and Volunteers Working with Children	9
10	Guidance for All Other NDCS Staff, Managers and Volunteers	9
11	Key Responsibilities of Parents and Carers	9
12	Key Responsibilities of Children and Young People	10
13	Dealing with E-Safety Incidents	10
14	Accidental or deliberate access to inappropriate material	10
15	Accidental or deliberate access to illegal material	11
16	Inappropriate use of email or other technologies	11
17	Illegal use of email and other technologies	11
18	Deliberate misuse of the network	11
19	Bullying or harassment using technologies	11
20	Sexual Exploitation using technologies	11
21	Reporting	12
	Appendix 1 Additional Advice for NDCS Staff and Volunteers Working with Children and Young People	13
	Appendix 2 CEOP Top Tips for Parents and Carers	15

E-Safety
(Safer Working Practice with Technology)

1. Introduction

1.1 New technologies offer huge benefits for all children and young people and for deaf children and young people in particular. At times, in using new technologies, children and young people will encounter risks. It is now widely understood that the risks are posed more by the behaviour of children and adults than by the technologies themselves.

1.2 The Byron review classifies e-safety risks as involving content, contact and conduct, illustrating that the risk element in using new technologies is often determined by behaviours rather than the technologies themselves[1].

	Commercial	**Aggressive**	**Sexual**	**Values**
Content Child as recipient	Adverts Spam Sponsorship Personal information	Violent/hateful content Misleading info	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice
Contact Child as participant	Tracking Harvesting personal info	Being bullied or harassed	Meeting strangers Being groomed	Self harm Unwelcome persuasions
Conduct Child as actor	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying/harassing another	Creating and uploading inappropriate material	Providing misleading info/advice

1.3 Therefore NDCS approach to e-safety (safer working practice with technology) will focus on developing safe and responsible behaviours, as part of its framework of e-safety measures.

1.4 This policy is intended to inform staff, managers, volunteers and parents as well as children and young people about what is expected of them as well as about how NDCS will help to safeguard them. It is intended to:

- Assist adults to work safely and responsibly and monitor their own standards and practice in using technology
- Help adults set clear expectations of their own behaviour and comply with codes of practice

[1] Table developed by the EUKids Online project and referenced in paragraph 1.3 of the Byron Review. www.dcsf.gov.uk/byronreview/pdfs/Final

- Minimise the risk of allegations being made inappropriately

- Give a clear message that unlawful or unsafe behaviour is unacceptable and that where appropriate disciplinary action will be taken

- Support managers, staff and volunteers in establishing a culture of technology use that safeguards children and young people as well as staff and volunteers

- Support staff and volunteers in following the Acceptable Use Policy

2. Policy Statement

2.1 NDCS believes that the safety of children is a priority. All children are entitled to be protected when receiving services from NDCS and its partner organisations.

2.2 E-safety (safer working practice with technology) is the responsibility of all NDCS managers, staff and volunteers.

2.3 Communication between children and adults by whatever method should take place within clear and explicit boundaries. This includes wider use of technology such as mobile phones, text messaging, email, digital cameras, videos, webcams, websites and blogs.

2.4 In general, the way that adults should conduct themselves with children and young people is no different when using technology than when dealing with them face to face.

2.5 NDCS will report any possible offences or online child protection issues to the relevant authorities including the Police, Child Exploitation and Online Protection (CEOP), Action Fraud, the Local Authority Designated Officer (LADO) or managing allegations process and the Disclosure and Barring Service.

2.6 For more detail about the standards of behaviour expected by NDCS of its managers, staff and volunteers, the NDCS policy **Safer Working Practice for Adults Working with Children**, **NDCS volunteer procedures** and the **Social Media Policy** should be consulted.

2.7 NDCS should, if possible, support children and young people to establish e-safety skills, which will ultimately help protect children as they grow and mature, regardless of how the technology and risks evolve.

3. Areas of Concern[2]

3.1 As the use of technology increases, the importance of positive online behaviours increases.

3.2 Social networking provides a good example of how online behaviour can present e-safety risks. This is extremely popular with children and young people, and encourages users to be creative users of the internet rather than just passive consumers. Users can express themselves with online personalities, chat and socialise with peers, and publish and share multimedia content such as music, photos and video clips with others.

3.3 If basic e-safety advice (such as that found in Appendices 1and 2) is followed, social networking poses little risk. However, if used inappropriately, many risks can be present for the user, and others:

- People may upload content that is inappropriate, offensive or even illegal to their online spaces, posting material that could damage their reputations or the reputations of others, or breach intellectual property rights.
- Posting inappropriate comments to the profiles of others can result in bullying or humiliation for the target, or potential charges of libel for the perpetrator.
- Although most social networking sites enable a profile to be set to private and only viewed by approved contacts, many users do not apply them.
- Maintaining very detailed online profiles, including personal information, photos and accounts of daily routines can lead to users being identified or contacted in person.
- Most social networking sites set age restrictions on using their services, but there is no way of authenticating users. As a result, many younger children disregard the terms and conditions of the service, unaware of the risks this might pose.
- Once posted online, a photo or video clip can be freely copied, manipulated and circulated and will potentially exist forever.
- At its worst, in cases of online bullying, harassment or abuse, the inability to permanently remove online content and images can further add to the suffering of the target. Less damaging but equally impossible to remove, content posted in the naivety of youth could embarrass individuals in years to come.
- Young people have been known to post sexually explicit photos of themselves online, but those involved in such activities (or those forwarding such images to other recipients) could unknowingly be committing child sex abuse offences if the subject of the photo is, or appears to be, under the age of 18.
- Technology offers a perceived anonymity that may lead people to participate in abusive behaviours online that they would not contemplate in the real world.
- In cyber bullying, the target is potentially vulnerable 24:7 and no longer has a safe haven away from the bully; malicious or defamatory content can be circulated with ease, may be seen by a much wider audience, and will potentially exist forever despite best attempts to remove it.

[2] AUPs in Context, BECTA, Feb. 2009

4. Protecting Staff and Volunteers

4.1 Adults have a duty to protect the children in their care, but they are also susceptible to risks.

4.2 There are many recent reports of teachers being harassed or intimidated using new technologies, both in and out of the classroom.

4.3 Equally, there are reported instances of childcare professionals compromising their professional reputation through social networking sites and other forms of media, or using work networks to access or circulate inappropriate or illegal content.

4.4 Establishing safe and responsible online behaviours throughout the organisation will help to protect adults and will help to maintain the reputation of NDCS.

5. Responsibilities of All Technology Users

5.1 All users must familiarise themselves with and follow the NDCS Acceptable Use Policy and its associated policy documents and this e-safety policy.

5.2 All managers, staff and volunteers are expected to comply with the following:

- All users should familiarise themselves with and follow the Acceptable Use Policy and its associated policy documents and this e-safety policy.

- All managers, staff and volunteers must take responsibility for their own use of new technologies, making sure that they use technology safely, responsibly and legally.

- All managers, staff and volunteers must take personal responsibility for their awareness of the opportunities and risks posed by new technologies.

- No communications device, whether NDCS provided or personally owned, may be used under the auspices of NDCS for the bullying or harassment of others in any form.

- No applications or services accessed by managers, staff or volunteers may be used to bring NDCS, or its members, into disrepute.

- All managers, staff and volunteers have a responsibility to report any known misuses of technology, including the unacceptable behaviours of others.

- All managers, staff and volunteers have a duty to respect the technical safeguards which are in place. Any attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services, is unacceptable.

- All managers, staff and volunteers have a duty to report failings in technical safeguards which may become apparent when using the systems and services.

- All managers, staff and volunteers have a duty to protect their passwords and personal network logins, and should log off the network when leaving workstations unattended. Any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

- All managers, staff and volunteers should use network resources responsibly. Wasting effort or networked resources, or using the resources in such a way so as to diminish the service for other network users, is unacceptable.

- All managers, staff and volunteers should understand that network activity and online communications are monitored, including any personal and private communications made via the NDCS network.

- All managers, staff and volunteers should be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action.

- All users must take responsibility for reading and upholding the standards laid out in this policy

- All users should understand that the policy is regularly reviewed and consistently enforced.

- Managers, staff and volunteers thought to be in breach of this policy will be dealt with under NDCS Disciplinary Procedures and NDCS Volunteer Procedures.

- NDCS will report activity or actions which place children and young people at risk to the appropriate authorities

5.3 Teams within NDCS will need to develop their own guidance to meet the different circumstances of their work with children and young people.

6. Key Responsibilities of senior management

- Developing, owning and promoting the e-safety policy to all stakeholders.
- Supporting the Designated Manager, Designated Persons, Digital and IT Teams in the development of an e-safe culture.
- Making appropriate resources available to support the development of an e safe culture.
- Receiving and regularly reviewing reports of e-safety incidents
- Supporting Designated Persons, Digital and IT Teams in the appropriate escalation of e-safety incidents.
- Taking ultimate responsibility for e-safety incidents. The management team will need to take ultimate responsibility for any e-safety incidents which do occur.
- Reading the Acceptable Use Policy, its associated documents and this e-safety policy and adhering to them

- Maintaining a professional level of conduct in their personal use of technology, both in work and outside of the work environment.
- Taking personal responsibility for their professional development in this area.

7. Key Responsibilities of the Designated Manager and Designated Persons

- Developing an e safe culture under the direction of the management team and acting as a named point of contact on all e-safety issues.
- Leading the promotion of e-safety with input from all stakeholder groups.
- Promoting the e-safety policy to all stakeholders, and supporting them in their understanding of the issues.
- Ensuring that e-safety is embedded within continuing professional development (CPD) for managers and staff and co-ordinating training as appropriate.
- Ensuring that e-safety is embedded across activities for children and young people as appropriate.
- Ensuring that e-safety is promoted to all users of network resources.
- Maintaining a record of e-safety incidents
- Monitoring and reporting on e-safety issues to the management team, and other agencies as appropriate.
- Developing an understanding of the relevant legislation.
- Liaising with other agencies as appropriate.
- Reviewing and updating e-safety policies and procedures on a regular basis.
- Reading the Acceptable Use Policy and its associated policy documents and this e-safety policy and adhering to them
- Maintaining a professional level of conduct in their personal use of technology, both in work and outside of the work environment.
- Taking personal responsibility for their professional development in this area.
- This is to be incorporated into the job descriptions of Designated Persons.

8. Key Responsibilities of the IT Teams

- Supporting the Designated Manager and Designated Persons in the development and implementation of appropriate e-safety policies and procedures
- Ensuring that the safeguarding of children and young people is given priority in the development and implementation of Acceptable Use Policies
- Providing a technical infrastructure to support e safe practices
- Taking responsibility for the security of systems and data.
- Reporting any technical breaches to the appropriate Executive Director, and taking appropriate action as advised.
- Developing an understanding of the relevant legislation as it relates to the technical infrastructure.
- Liaising with other agencies as appropriate.
- Maintaining a professional level of conduct in their personal use of technology, both in work and outside of the work environment.
- Taking personal responsibility for their professional development in this area.
- This is to be incorporated into the relevant job descriptions.

9. Key Responsibilities of NDCS Managers, Staff and Volunteers Working with Children

- Championing the development of e-safety policies.
- Adhering to the Acceptable Use Policy and its associated policy documents and this e-safety policy
- Taking responsibility for the security of systems and data.
- Having an awareness of e-safety issues, and how they relate to the children in their care or with whom they have contact through their work with NDCS
- Modelling good practice in using new and emerging technologies, emphasising positive learning opportunities rather than focusing on negatives.
- Identifying individuals of concern and taking appropriate action.
- Knowing when and how to escalate e-safety issues.
- Maintaining a professional level of conduct in their personal use of technology both in their professional and their personal roles..
- Taking personal responsibility for their professional development in this area.

10. Guidance for all other NDCS Staff, Managers and Volunteers

All other NDCS managers, staff and volunteers should:

- Take responsibility for the security of systems and data.
- Have an awareness of e-safety issues, and how they relate to children
- Observe good practice in using new and emerging technologies.
- Identify individuals of concern and take appropriate action.
- Know how and when to escalate e-safety issues.
- Maintain a professional level of conduct in their personal use of technology, both in work and outside of the work environment.
- Take personal responsibility for their professional development in this area.

11. Key Responsibilities of Parents and Carers

It is important to recognise that parents and carers play a key role in ensuring the safety of children and young people

- Discussing e-safety issues with their children and reinforcing appropriate behaviours at home.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Modelling appropriate uses of new and emerging technology.

11.1 NDCS managers, staff and volunteers can support parents and carers in this by providing appropriate advice. (See also Appendix 2 CEOP top tips for Parents and Carers)

12. Key Responsibilities of Children and Young People

Children and young people play a part in ensuring their own safety by:

- Taking responsibility for keeping themselves – and others – safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.
- Respecting the feelings, rights, values and intellectual property of others.
- Seeking help from a trusted adult if things go wrong, and supporting others who may be experiencing e-safety issues.
- Discussing e-safety issues with parents and carers in an open and honest way.

12.1 Managers, staff and volunteers may wish to have additional guidance for use with children and young people. See Appendix 1 Additional Advice (for NDCS managers, staff and volunteers to use with children and young people).

13. Dealing with E-Safety Incidents

13.1 Depending on the nature of the event, different e-safety incidents will require different responses, and undoubtedly no two e-safety incidents will be exactly the same.

13.2 E-safety incidents should be dealt with according to the procedure defined in the Acceptable Use Policy and its associated documents.

13.3 Any incident which may have compromised the safety of a child or young person must also be dealt with in line with the Child Protection Policy and must include consultation with the Designated Person, Designated Manager and Child Protection Advisor.

14. Accidental or deliberate access to inappropriate material

14.1 The definition of ‘inappropriate’ may change according to the user or the setting. Inappropriate material is anything which is illegal or encourages exploitation of children or young people. Managers and staff should consult the NDCS Safer Working Practice Guidance for details of inappropriate activity. Volunteers should consult the Volunteer Handbook. Where there is any doubt, managers and staff should consult their line manager or Designated Person. Volunteers should consult their manager or project leader. Disciplinary sanctions will apply where any action places children or young people at risk. Different approaches may be necessary depending on whether the access was accidental or deliberate. Managers and staff should also be familiar with and follow the Acceptable Use Policy and its associated policy documents. Volunteers should consult the Volunteer Handbook or their manager or project leader.

15. Accidental or deliberate access to illegal material

15.1 This applies to all access whether at home, at work and regardless of ownership of equipment. Managers and staff should also be familiar with and follow the Acceptable Use Policy and its associated policy documents.

15.2 If illegal material is accessed, escalation of the incident will be necessary.

16. Inappropriate use of email or other technologies

16.1 Inappropriate use is anything which is illegal or encourages exploitation of children or young people. Staff and managers should consult the Safer Working Practice Policy for details of inappropriate activity. Volunteers should consult the Volunteer Handbook. Where there is any doubt, managers, staff and volunteers should consult their line manager or Designated Person.
Managers and staff should also be familiar with and follow the Acceptable Use Policy and its associated policy documents.

17. Illegal use of email and other technologies

17.1 Illegal use of email and other technologies should always be escalated to an appropriate agency.
Managers and staff should also be familiar with and follow the Acceptable Use Policy and its associated policy documents.

18. Deliberate misuse of the network (for example, hacking, virus propagation or circumventing safety controls)

18.1 Managers and staff should consult the NDCS Acceptable Use Policy and its associated policy documents about inappropriate use of network resources, the monitoring that is in place and the sanctions which will apply to deliberate misuse. If networks have been used for illegal activity, the incident should be escalated accordingly.

19. Bullying or harassment using technologies

19.1 Bullying or harassment is not acceptable in any circumstance, via any means. Managers and staff should also be familiar with and follow the Acceptable Use Policy and its associated policy documents.

20. Sexual exploitation using technologies

20.1 This is a serious offence, and will require escalation to appropriate external agencies as necessary.

20.2 Managers and staff should also be familiar with and follow the Acceptable Use Policy and its associated policy documents.

21. Reporting

21.1 All breaches should be reported to the line manager and to the Designated Manager or Designated Person where a child's safety has been or may have been compromised.
Serious breaches will be reported to the Executive Directors for Children Young People and Families and for Finance and Administration

21.2 The Designated Manager and Child Protection Advisor will consult with the ICT Manager about the technical aspects of breaches of this policy.

21.3 NDCS will report any possible offences or online child protection issues to the relevant authorities including the Police, Child Exploitation and Online Protection (CEOP), Action Fraud, the Local Authority Designated Officer (LADO) or managing allegations process and the Disclosure and Barring Service.

Appendix 1

Additional Advice (for NDCS managers, staff and volunteers to use when working with children and young people)

The following is useful advice for children and young people to follow:

For Young Children

Think before you click
I will only use the Internet and email with an adult
I will only click on icons and links when I know they are safe
I will only send friendly and polite messages
If I see something I don't like on a screen, I will always tell an adult

For Young People

These rules will keep me safe and help me to be fair to others.

- I will keep my logins and passwords secret.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

What to do if you are worried [3]

- If someone makes you feel uncomfortable, talk to an adult you trust, such as a relative or teacher. If you would prefer to talk to someone in confidence you can contact Childline (0800 1111).
- If someone has acted inappropriately online towards you, or someone you know, you can report directly to the Child Exploitation and Online Protection Centre (CEOP). It could be sexual chat, being asked to do something that makes you feel uncomfortable or someone asking to meet up.
- If someone is bullying you, there is help and support available from CyberMentors

[3] NB Not all of these resources are accessible by deaf children and young people.

- If someone is bullying you using your information, there is help and support available from CyberMentors and BeatBullying
- Know what to do if something online has upset you: talk to Childline or the Samaritans if you are feeling desperate or sad, B-eat for eating disorder advice and go to Report-it to report incidents of race hate.
- You can also report to NDCS if our terms of service have been broken
- Illegal child sex abuse images online can be reported to the Internet Watch Foundation (IWF) or your local police.
- You can report fraud or online scams or viruses to Action Fraud – the UK's national fraud reporting centre
- Get Safe Online provides advice on how people can use the internet confidently, safely and securely

Appendix 2

CEOP Top Tips for Parents

- Be involved in your child's online life. For many of today's young people there is no line between the online and offline worlds. Young people use the internet to socialise and grow and, just as you guide and support them offline, you should be there for them online too. Talk to them about what they're doing, if they know you understand they are more likely to approach you if they need support. Watch Thinkuknow films to learn more. The Thinkuknow programme has films and advice from five all the way to 16. Your child may have seen these at school, but they can also be a good tool for you to find out more about what young people do online and some of the potential risks.

- Keep up-to-date with your child's development online. Be inquisitive and interested in the new gadgets and sites that your child is using. It's important that as your child learns more, so do you.

- Set boundaries in the online world just as you would in the real world. Think about what they might see, what they share, who they talk to and how long they spend online. It is important to continue to discuss boundaries so that they evolve as your child's use of technology does.

- Know what connects to the internet and how. Nowadays even the TV connects to the internet. Your child will use all sorts of devices and gadgets; make sure you're aware of which ones can connect to the internet, such as their phone or games console. Also, find out how they are accessing the internet – is it your connection or a neighbour's Wi-Fi? This will affect whether your safety settings are being applied.

- Consider the use of parental controls on devices that link to the internet, such as the TV, laptops, computers, games consoles and mobile phones. Parental controls are not just about locking and blocking, they are a tool to help you set appropriate boundaries as your child grows and develops. They are not the answer to your child's online safety, but they are a good start and are not as difficult to install as you might think. Service providers are working hard to make them simple, effective and user friendly.

- Emphasise that not everyone is who they say they are. Make sure your child knows never to meet up with someone they only know online. People might not always be who they say they are. Make sure your child understands that they should never meet up with anyone they only know online without taking a trusted adult with them.

- Know what to do if something goes wrong. Just as in the offline world, you want to help your child when they need it. Therefore, it is important to know when and how to report any problem.

- Further advice is available from ceop
  http://ceop.police.uk