Gateshead local safeguarding children board

MULTI-AGENCY

E-SAFETY GUIDANCE

SEPTEMBER 2010

CONTENTS

APPENDICES

1. Introduction

The protection of children and young people has always been a core commitment of all partners who work together in Gateshead. The vision of Gateshead Local Safeguarding Children Board (LSCB) is that every child should grow up in a loving and secure environment, which is free from abuse, neglect and crime enabling them to enjoy good health and fulfill their social and educational potential.This vision should extend to the digital world, every young person should be confident and safe in the digital world and be supported and encouraged to develop as positive role modes and responsible 21st century citizens.

Adults working with children need to ensure that they are competent, confident and safe when working with new technology. This is particularly relevant to those working in a school setting, but also to adults working as carers or in a caring profession, for example foster carers or social workers. Many adults are unsure or anxious in their approach to new technology, and the "digital world" that young people now inhabit is very different from to the world that most professionals grew up in. Where once the desktop computer was the only way to access the internet, many young people can now access the virtual world via laptops, mobile phones and games consoles. Technology offers children and young people unprecedented opportunities to learn, communicate, discover and create however there are some inherent risks. Most young people's confidence and competence in using the technologies is high, however their knowledge, awareness and understanding of the risks may be less so.

Safeguarding children in both the real and virtual world is everyone's responsibility. This document discusses appropriate and safer behaviours for adults to protect themselves whilst also protecting children from risk.

The author would like to thank South Tyneside Safeguarding Children Board for sharing literature, which is used in this document and also Northumberland Safeguarding Children Board.

2. Background

Much of the early work on e-safety focussed on schools, as they are one of the key places where children accessed computers. But as access to technology has grown the focus has had to expand. E-safety is now seen as a key safeguarding issue and one that rests with LSCBs.

It is considered an essential part of the duty on agencies under section 11 of the Children Act 2004 to safeguard and promote the welfare of children. E-safety is mentioned in Working *Together to Safeguard Children* (2010*)*. It is a key part of the Staying Safe Action Plan ('Addressing new threats to children's safety') which includes a commitment from the government to give 'full and proper consideration to, and respond to the recommendations of the Byron Review.

The British Educational Communications and Technology Agency (Becta), the government agency that leads on much of this work, is focussed on ensuring there are local strategies in place to address e-safety. They have produced extensive guidance and support materials including the key publication 'Safeguarding children in a digital world' (2008).

3. What is e-safety?

E-safety is about applying the lessons we have learnt about keeping children, young people and adults safe in the digital world.

E-safety is a way of behaving, working, and practicing. It is part of being a responsible parent, child, or member of staff, of being a positive role model and a responsible 21st century citizen. It is key because many aspects of our lives are directly shaped by technology.

From September 2010 e-safety will be a compulsory part of the curriculum for all children from age five.

4. Why have e-safety policies or guidance?

The growth of computer/digital-based technology has opened up enormous opportunities for improving children's ability to enjoy and achieve. Personal computers and mobile phones are now central parts of young people's lives and are focal points for learning and social activities. However, the technology that provides children and young people with so much opportunity also creates a new set of safeguarding challenges. Access to the Internet and digital forms of communication mean that children and young people are at increased risk of sexual exploitation, bullying, exposure to indecent images, grooming, inappropriate advertising and many other influences that may put their safety and welfare in jeopardy.

Professionals working with young people need to ensure that these young people are safe, not just in school, but are prepared for the outside world including in the home and in the community.

The need to safely maximise the positive opportunities made possible by new technology is the driving force behind the concept of e-safety. Work on e-safety is not new. There has been widespread concern and action regarding images of child exploitation and abuse ('child pornography'). LSCBs have sought to address this. But as technology has grown, so has the problem and we need to be ready to act and that is why we need clear policies and procedures.

5. What does this guidance cover?

E-safety is concerned with behaviour that can be illegal or inappropriate, whether deliberate or accidental. This could include the danger of terrorists using the internet to indoctrinate young people into violent extremism through to the impact of an inappropriate email or an image on a social networking site.

The guidance is primarily focussed on safeguarding children, but adults (staff, parents, carers, volunteers) also need to consider the use of technology and how this impacts upon children and young people. E-safety must be the concern of all adults; even those that do not use digital technology themselves need to know how to keep their children or grandchildren safe in the digital world.

E-safety addresses the safeguarding concerns that we have been working on for many years. It is about recognising how technology impacts upon these issues and how it can be used to harm others. We need to adapt and develop our policies and procedures to take account of digital technology and its impact on safety and safeguarding. The issues themselves are not new, just the environment in which they take place. Our strategy is about making sure we are ready to deal with the changing face of safeguarding.

Some of the typical concerns include:

- Cyber bullying
- Identity theft
- Grooming
- Inappropriate and illegal images
- Fraud

We need to think about how we all use technology as positive, responsible 21st century citizens. The anonymity and remoteness we can feel when on line or using digital technology can allow us to drop our guard and our standards.

E-safety principles must be applied to the use of computer and digital technologies in the broadest sense. That is the use of:

- Computers – desktops, laptops, palm tops, games consoles
- Mobile phones
- Digital cameras
- Video/computer games
- Email and other forms of digital communication
- Use of the internet (browsing, downloading, uploading)

It covers the use of these tools and techniques at work and at home. We must consider, 'what are the rules governing the use of this technology in this setting', 'what are the expectations upon me' and 'what will be the outcome'.

Whilst technology is central to this work, it is important to clarify that the work is part of a safeguarding rather than a technical agenda.

6. What is the aim of this guidance?

- To provide children, young people, parents/carers and staff with the knowledge and skills they require to safeguard themselves and others in the digital world
- To ensure that all people who work with children and young people have access to good quality procedures and effective training to safeguard against the risks of online activity
- To ensure that systems and services are in place to identify, intervene and divert people engaging in any form of illegal, inappropriate or harmful behaviour online and offline.

7. Who does this guidance apply to?

Gateshead LSCB has approved this strategy. It is directed particularly at those agencies with duties to safeguard and promote the welfare of children under section 11 of the Children Act 2004 or section 175 of the Education Act 2002. However it also stands as guidance to all agencies in all sectors in Gateshead. Each agency will need to interpret this guidance relative to the services they provide, the degree to which they have direct contact with children and the extent to which they work with children using digital technology.

All agencies will need to have appropriate arrangements:

- That govern staff use of digital technology. This may include consultants, temporary and agency staff and those working from home.
- Governing how visitors use digital technology when on site at one of their buildings, such as a person visiting a hospital with a mobile phone with a digital camera and access to the Internet.
- Governing how staff and visitors use their personal digital technology, such as laptops, mobile phones whilst at work or at home. This touches upon the concept of suitability within the children's workforce. Those who access child abuse images at home are no more suitable to work with children than those who access them at work.

Agencies that work directly with children and families and especially those that provide access to digital technology for children and families, such as schools, youth clubs, libraries, hospitals and other settings, will need to ensure they have arrangements in place governing how children and families use technology provided by or through them.

All agencies / schools should undertake a risk assessment concerning access to and the use of digital technology to ensure they have appropriate arrangements in place.

This strategy cannot cover and does not attempt to cover all arrangements for schools and agencies working in Gateshead. It is to be seen as guidance to help inform what local agencies need to do to ensure they are equipped to safeguard and promote the welfare of children in a digital age. The expectation is that each school and agency will have or will develop policies and procedures to address e-safety in their setting. These individual polices must be consistent with this strategy and the Gateshead LSCB Inter-agency Child Protection policy

Gateshead LSCB has two key objectives:

- To co-ordinate local arrangements for safeguarding children
- To ensure local arrangements for safeguarding children are effective

It is the LSCB's responsibility to ensure appropriate guidance is in place, to support agencies to develop their own arrangements and to monitor the impact of these arrangements to make sure they are effective.

However, each individual agency and school retains its own responsibility and accountability for fulfilling their duties to safeguard and promote the welfare of children. As such they must develop the policies, processes and practices required to meet this duty and in doing so they will need to consider the impact of their policies and practices on children, parents/carers and staff.

8. Expectations upon agencies, schools and Gateshead LSCB

Each agency / school will have a named person / lead for e-safety, who should:

- Have a remit for safeguarding within the agency
- Have an awareness of e-safety / challenges posed by technology
- Have an interest in children and young people's use of digital technology
- Be familiar with safeguarding practices including the use of multi-agency procedures
- Be able to receive e-safety concerns and ensure agreed procedures are followed
- Have a commitment to multi-agency working

Policies, procedures and practices

- All agencies / schools in Gateshead should have policies, procedures and practices in place governing the acceptable and safe use of digital technologies relevant to the services they provide. This includes the appointment of named / lead people for e-safety.
- All policies, procedures and practice guidance related to the safe use of digital technology, **except AUPs**, must be reviewed and updated at least every 3 years or following any incident or development which questions the effectiveness of procedures. **It is recommended that AUPs be reviewed annually.**
- Gateshead LSCB must ensure there is a clear and agreed process across all agencies / schools for identifying and reporting e-safety concerns and to make it inclusive of the Internet Watch Foundation and CEOP as well as Northumbria Police
- All agencies / schools must ensure they use Gateshead LSCB's media strategy when dealing with media enquires into child protection incidents whether involving digital technology or not.

Education, training and raising awareness

- All agencies / schools must make arrangements for the provision of consistent and high quality training on e-safety, which is regularly updated relative to the services they provide.

Gateshead LSCB will monitor this as part of its remit to ensure local agencies are fulfilling their duties to safeguard and promote the welfare of children.

- Gateshead LSCB must ensure that its multi-agency training programme includes e-safety training to support agencies in understanding how they work together to safeguard children in a digital world.
- Gateshead LSCB, schools and agencies (subject to the services they provide) must ensure that children, young people, parents and carers have access to education and training that will promote safe and responsible use of the Internet and other digital technologies.
- Gateshead LSCB, schools and agencies (subject to the services they provide) must ensure that e-safety is the subject of awareness raising campaigns that will enable parents and carers, the media and partner agencies to recognise the opportunities and the threats of the Internet and digital technologies.

Infrastructure and technology Objectives

- Gateshead LSCB must ensure there is robust guidance and standards to support agencies in providing safe Internet provision. This must include national standards on filtering and accreditation of software.
- All agencies / schools must have safe technological infrastructures, including an appropriately approved Internet Service Provider and systems for filtering, monitoring and recording Internet and Intranet activity.
- Gateshead LSCB must develop and disseminate good practice information to other providers (such as post offices, internet cafés, phone boxes, digital handheld devices and mobile phones) aimed at enabling children and young people to use the Internet safely and responsibly.
- Gateshead LSCB must support national work focused on bringing together digital technology companies and statutory agencies to consider new and emerging technologies and their trends, and to disseminate good practice as quickly as possible to agencies providing services to children, young people and their families.

Inspection and standards Objectives

- All individual agencies / schools must have data recording systems and processes to identify e-safety policies and practices in place and how they are reviewed and developed. Agencies must also keep records of e-safety concerns that can be used to support the review and development of polices and practices.
- Gateshead LSCB must develop a framework which includes policies, practices and procedures; organisational Internet safety reporting mechanisms; infrastructure arrangements and training. This will enable Gateshead LSCB must have oversight of the development of e-safety policies, procedures and practices within agencies in Gateshead.
- Gateshead LSCB, schools and agencies (subject to the services they provide) should that ensure children and young people are involved in the development and review of policies and practices relating to e-safety and safeguarding in general.

9. Key requirements for policies, practices, infrastructure and inspection

9.1 Policies, procedures and practices

Schools and agencies (subject to the services they provide) must have:

- A risk assessment identifying access to and the use of digital technology

- An e-safety policy
- Acceptable use polices (see appendix B) covering relevant forms of technology and settings signed by:
    - Staff
    - Children and young people
    - Visitors
- An agreed process for responding to e-safety concerns (see section 4)
- An e-safety log for recording all e-safety concerns, actions taken and outcomes

9.2 Infrastructure & Technology

All agencies and schools must:

- Ensure access to internet is provided by an appropriate approved supplier
- Have appropriate approved filtering / fire walls and controls
- Have systems for monitoring use / identifying breaches of AUP
- Systems to record & store all emails

9.3 Education, training & awareness

Schools and agencies (subject to the services they provide) must:

- Identify staff requiring training
- Plan to develop and deliver training to the identified staff covering:
- The development of all relevant policies and procedures such as AUPs and responding to e-safety concerns
- Safeguarding in the digital world
- Risks associated with the use of technology
- The role of staff / carers (as appropriate)
- Links to other relevant policies and procedures such as Allegations Management

In addition, the Gateshead LSCB training programme must cover:

- Inter-agency e-safety arrangements
- Inter-agency safeguarding arrangements
- E-learning package on e-safety

Gateshead LSCB, schools and agencies (subject to the services they provide) must make arrangements for the provision of training, guidance and information to children, young people, parents and carers covering:

- E-safety concerns
- Appropriate responses to e-safety concerns
- Sources of support and resources available for children, young people, parents and staff
- E-safety resources on Gateshead Council / Gateshead LSCB / Agency websites

9.4 Monitoring and review

- All policies and procedures should be dated and indicate the date of the latest review and the date of the next review.
- All policies and procedures, **except AUPs**, must be reviewed at least every three years with earlier reviews being triggered following incidents or developments that may diminish the

effectiveness of the policy or procedure. It is recommended that AUPs be reviewed annually.

- All agencies should maintain an e-safety log to record all e-safety incidents / concerns
- Gateshead LSCB must develop and review an e-safety data monitoring set for agencies to use (see 9.5).
- Gateshead LSCB must make use of the data set to confirm the implementation of the strategy and measure its impact.

9.5 Monitoring impact

Gateshead LSCB will use the following indicators to measure the impact of the strategy and action plan:

- The number of agencies with AUPs less than one year old
- The number of agencies with an e-safety lead
- The number of individual agencies with procedures for responding to concerns
- The number of agencies using an accredited Internet Service Provider
- The number of agencies with a filtering and monitoring plan in place
- The number of agencies with an e-safety training plan
- The number of training events per agency
- The number of agencies with an awareness raising / public information plan
- Gateshead LSCB may at any time request reports from agencies regarding the performance of their e-safety systems.

10. Useful Links

1. Gateshead LSCB Website – www.gateshead.gov.uk/lscb
2. Child Exploitation and Online Protection Centre is a law enforcement agency. www.ceop.gov.uk
3. Thinkuknow – online safety for young people and parents – www.thinkuknow.co.uk
4. Insafe – a Europe wide e-safety service – www.saferinternet.org
5. Internet Watch Foundation – a hotline for reporting illegal online content www.iwf.org.uk
6. Kidscape – a UK charity committed to keeping children safe www.kidscape.org.uk
7. Childnet, a non-profit organisation working to help make the Internet a great and safe place for children. www.childnet-int.org
8. 'Safeguarding Children in a digital world' and other guidance is available from www.becta.org.uk
9. Cyber bullying [http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_ob_03]
10. Virus prevention and protection [http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pys_pat_03&rid=14874]
11. Acceptable use policy (AUP) [http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_aup_03]
12. AUPs in context – Establishing safe and responsible online behaviours http://schools.becta.org.uk/index.php?section=is&&catcode=ss_to_es_tl_rs_03&rid=16252
13. Reporting incidents [http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_aup_03&rid=12002]
14. The Byron Review - http://www.dcsf.gov.uk/ukccis/userfiles/file/FinalReportBookmarked.pdf

APPENDIX A

Gateshead local safeguarding children board

E-safety
Model Policy for agencies and schools

Introduction

Safeguarding children is everyone's responsibility and for that reason statutory agencies and bodies such as local authorities, hospitals and schools are required to demonstrate their commitment to safeguarding children from those who may wish to deliberately harm them.

There is a clear expectation that such agencies have child protection and safeguarding policies in place that are consistent with the local multi-agency procedures agreed by the Local Safeguarding Children Board. This expectation also applies to other organisations, such as local community or faith based groups who work with children or provide services to them.

We now live in a digital world. Technology has changed how we live our lives. These facts mean that we must also update our approach to safeguarding children.

Many of the risks that exist for children in the 'real world' exist and can be exacerbated within the digital world. The expectation upon agencies, schools and community groups now includes safeguarding children in the digital world and it is vital that we all have the right policies, procedures and practices in place to achieve this crucial goal.

How to use this guidance

While there is no uniform e-safety policy that will suit all the policy should cover all potential / actual users of digital technology such as staff and visitors as well children and young people. It should also cover all types of technology such as computers, laptops, mobile phones and digital cameras.

This guidance sets out the core aspects of an e-safety policy and information on what each agency or body needs to have in place. You should use this to help develop your own policy that addresses your particular service and setting. Most of the headings given below are applicable to all agencies and schools and so should feature in your policies. Some of you may need to address areas not covered in this guidance. If there are any significant shortfalls in this guidance please contact the Gateshead Local Safeguarding Children Board.

This model policy has been developed in line with Gateshead LSCB e-Safety Guidance (2010) and follows the guidelines established by Becta.

Your e-safety Policy

Your policy should be located with or become part of your existing child protection / safeguarding policies. If it does not it should begin with cross-referencing to those policies, identifying e-safety as a key safeguarding concern. You should also confirm your commitment to safeguarding children, as demonstrated by the arrangements set out in your policy as described below.

1. Agency Commitment

Set out your agencies commitment to e-safety, mentioning planned developments, how e-safety has shaped service provision and how it will be a feature of your agencies development and overall approach to safeguarding.

2. Accountabilities & Responsibilities

Your agency should have **a lead officer for e-safety**. This should be someone with a safeguarding remit. The lead officer should be named in your policy along with a brief outline of his/her role and responsibilities. This might include developing e-safety tools and guidance, raising awareness of e-safety, training and education. The lead officer may have a particular role in liaising with lead officers from other agencies or schools to ensure a robust and consistent approach.

Your agency should have **a senior manager / representative** who has strategic lead for e-safety. This should demonstrate that e-safety is a priority and that there is a clear chain of accountabilities for e-safety and any e-safety concerns that arise.

Children, staff, parents or other interested parties should be able to contact these people to discuss concerns or share information.

3. Policies & Practices

Identify the e-safety guidance you already have in place or which is under development (including the completion date). This must include:

- An acceptable use policy or separate policies for different users (staff, young people, visitors) See appendix B of this document (Issued by CLC in respect of Schools and Council users)
- Staff / student / service user code of conduct (See Appendix C)
- A policy for responding to e-safety safeguarding concerns - including relevant contacts within your agency and in other key agencies such as Police and Children's Services. (See Appendix D)
- Risk assessment procedures / completed risk assessments with regard to e-safety
- Recording policy – setting out how concerns / issues should be recorded

The policies must be cross referenced to other related policies such as:

- Child protection
- Bullying
- Allegations management
- Complaints
- Whistle blowing
- E-security
- Media management strategy

4. Infrastructure

Your policy should explain the steps you have and will be taking to promote e-safety. This should include filtering systems, firewalls and process for monitoring inappropriate use of technology.

Every effort should be made to ensure technology users are aware of the monitoring systems in place in order to divert unwanted behaviour and to avoid claims from technology users of inappropriate 'spying'.

5. Education

Your commitment to e-safety should include:

- Training and development for staff / volunteers
- Information and guidance for children and young people
- Information and guidance for parents / carers members of the community
- A commitment to dealing with e-safety through raising awareness

6. Systems for inspection and review

Your policy should explain how and when existing policies and e-safety tools will be reviewed and updated. It should identify other agencies that have a role in inspecting and monitoring local arrangements, such as Ofsted or the Health Care Commission.

7. Useful contacts and references

There are a lot of e-safety resources available to children, young people, parents and staff. These should be widely publicised as a means of offering extra support and alternative means of understanding more about e-safety.

APPENDIX B

Gateshead local safeguarding children board

Appendix B – Acceptable use policies (AUP)

Taken from "A guide for schools in developing an e-safety strategy" by Northern Grid for Learning.

Name of School / Agency	
Name of E safety Contact in School / Agency	
Endorsed by:	o Head Teacher / Chief Officer o Governors / Governing body o PTA / Service users o LSCB
Date of AUP	o
Review date	o
School / Agency Philosophy / Culture	o Safe Environment, respect for all, non tolerance of bullying o Work life balance – are there opportunities for personal use?
Applies to:	o Staff /Adults o Learners / service users o Visitors
Monitoring and reporting	o State what is monitored; email, computer records, Internet activity etc… o State what devices the AUP applies to, PCs, laptops, mobile phones, digital cameras etc… o Only approved devices to be connected to school / agency systems o Monitoring records are reviewed regularly and acted upon o Head /Chief Officer is included in reporting procedure o Have procedures in place to ensure systems manager knows what is connected and nature of all activity o Monitoring to extend to off site devices belonging to the school
Reporting Accidental Access	o Use an e safety book to log incidents and include reporting and action taken o Review filtering and access levels of users to minimise risk of recurrence of incident

Reporting Deliberate Abuse or	o Ensure adults and learners / service users know

Misuse	what action to take o Isolate device and have a clear procedure for protecting evidence o Notify key contacts in school, home and local authority where appropriate o Include guidance on illegal, inappropriate, indecent and bullying activities
Sanctions for misuse	Include policies for learners /service users and staff / adults **Students / service users** o Reprimand and guidance o Record incident o Sanction o Notify parent/carer and/or local authority **Adults** o Discipline and guidance o Record incident o Notify governing body o Notify local authority
Unlawful or Illegal Use	Any material or action which includes: o Child Abuse o Racial Hatred o Incitement to violence
What is inappropriate? (as determined by your AUP	This may vary for each of the key stages and type of school o Any text, image or file that may cause offence, distress o Wilful attempts to bypass security and access protocols o Spamming o Hacking o Impersonation
Anti Virus and Anti Spam	o Essential that all devices have appropriate protection o Violations are reviewed, reported and acted upon
Email	o School email account for school related use o Personal email accounts for personal use– do not display email addresses of others in the address bar when sending to multiple recipients o Language should be polite o No spam to be sent or forwarded o Understand the potential dangers of attachments and hyperlinks to websites

Internet Usage	**Downloading** o Access only to approved sites o Attempts to bypass will result in sanctions o Systems to report accidental access to inappropriate sites **Uploading** o No image, video or text without individual permissions o Parental permission required prior to displaying images and information on pupils on public facing websites
Copyright and Plagiarism	o No direct or indirect copying, reproducing or repurposing of material without acknowledgment and permission
Video Conferencing	o Use secure authenticated systems that are monitored o Learners should not be left unattended
Mobile devices	o Text o Bluetooth o Web access o Infrared o Virus protection o Connection protocols to ensure integrity of school systems and network o Monitoring procedure
Passwords	o Unique ID for all users where achievable o Always use password o Do not enable 'remember me' on devices o Log off device when leaving device unattended
Filtering	o Appropriate filtering for age group and adults o Monitor web activity and respond to violations o Update filtering rules regularly

Also see Becta's 'AUPs in context - Establishing safe and responsible online behaviours'

http://schools.becta.org.uk/index.php?section=is&&catcode=ss_to_es_tl_rs_03&rid=16252

APPENDIX C

Gateshead local safeguarding children board

Student / Young Person AUP

Students / young people are entitled to access to technology to help ensure that they can achieve their potential in their learning.

Students are not entitled to abuse technology by deliberately attempting to interfere with the performance of the school systems or devices belonging to other people.

Students are not entitled to use devices and Internet services to have a negative impact on other people. This includes cyber bullying of any members of the school community or inappropriate access to other people's files and documents on the school systems and the Internet.

- I will only access the system with my own login id and password, which I will keep secret
- I will not access other people's files
- I will only use the school devices and connectivity for school work and homework
- I will not bring to school any devices, to connect to the network or internet, from outside school unless I have been given permission
- I will ask permission from a member of staff before using the Internet;
- I will only E-mail people I know, or my teacher has approved
- The messages I send will be polite and responsible;
- I understand that it is not acceptable to post or upload images, of other people without their permission
- I will only use my own devices (including mobile phones PDAs etc) when permitted and only for activities acceptable to the school
- I will never arrange to meet someone or give any personal information over the Internet (name, address, telephone number, name and address of school, bank or credit card details).
- I will report any unpleasant material (including on the internet) or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself;
- Posting anonymous messages and forwarding chain letters is forbidden;
- I understand that the school may check my computer files and activity and may monitor the Internet sites I visit.

The AUP will need to cover other forms of technology such as mobile phones and digital cameras.

Gateshead local safeguarding children board

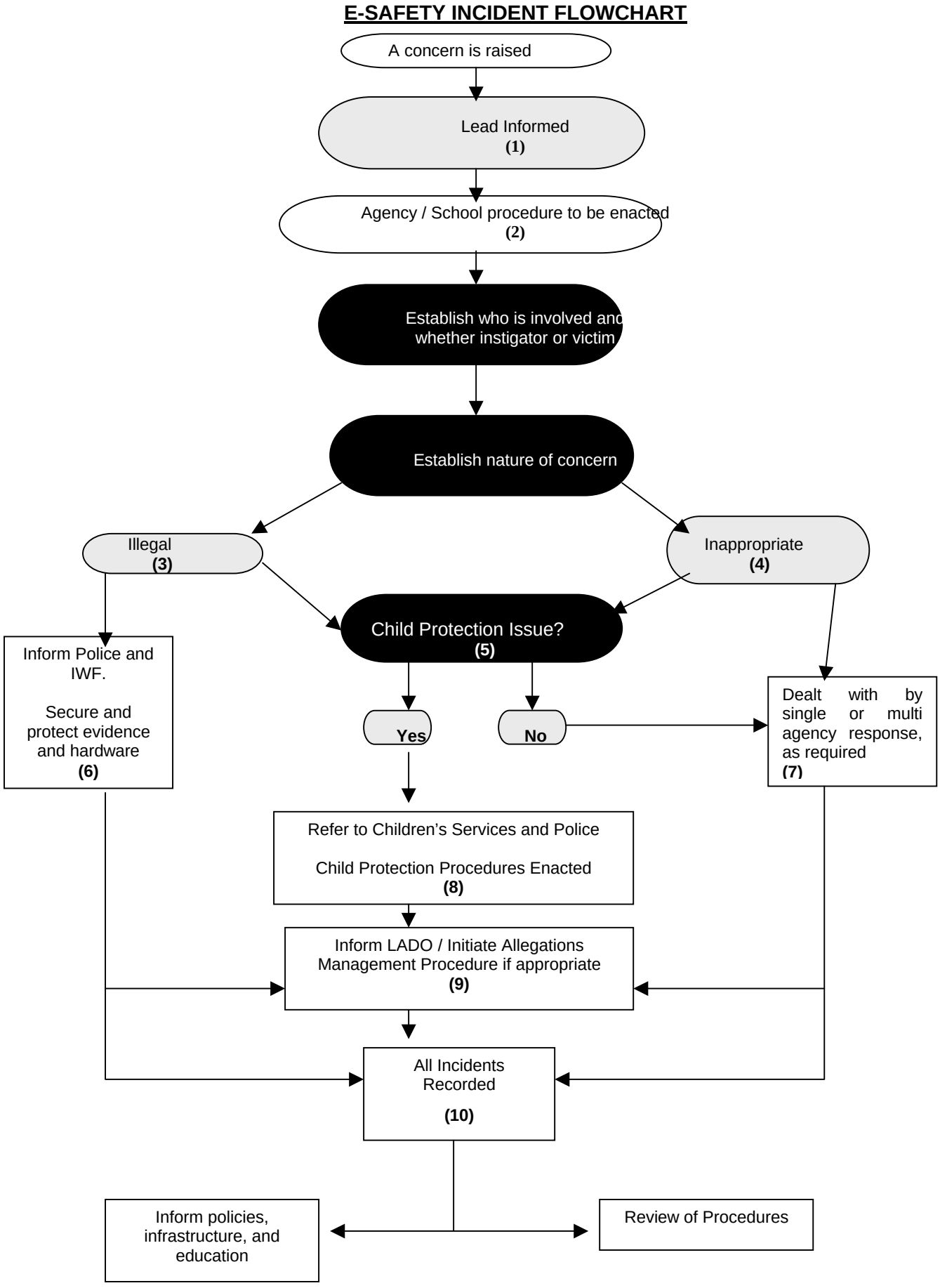
Staff / adults example AUP

All members of staff and other adults must understand and sign this AUP. The basic principle of this AUP is that the agency / school devices and connectivity may be used only to support the achievement of the school / agency objectives. Colleagues must ensure that they fully understand that the consequences of inappropriate activity can be severe leading to dismissal and criminal proceedings

- Personal use of the school's connectivity and devices is not permitted.
- No device will be introduced to school systems without ensuring it is free from malware, inappropriate/illegal content
- It is not permitted to use another person's log in details except in exceptional circumstances. On occasions when log ins are shared the details of this will be recorded in an e safety log or similar document.
- Images of students must be stored in designated area of school network within a time frame identified in the Digital Images Policy. It is not permitted to remove images off site (on camera, phone or storage device).

APPENDIX D

Responding to e-safety concerns



E-Safety Incident Flowchart – Guidance notes

One key aim of our work on e-safety is to embed e-safety into the existing polices and procedures for safeguarding children. The risks posed through the misuse of technology must be recognised and responded to as safeguarding issues. It is essential that Gateshead Local Safeguarding Children Board Safeguarding Procedures be adhered to. The procedures are available at **www.gateshead.gov.uk/lscb**

These notes relate to the flowchart above. The numbers on the flowchart correspond with the numbered guidelines below.

1. Gateshead LSCB recommends that all schools and agencies that have a safeguarding remit have a lead for e-safety. The lead will be responsible for the ensuring the agency/school has policies and procedures in place to identify and respond to e-safety concerns. The policies and procedures must be consistent with LSCB guidance. The lead will also have a role in liaising with other agency leads and the overall LSCB e-safety lead. The agency lead should:

    - Have a remit for safeguarding within the agency
    - Have an awareness of e-safety / challenges posed by technology
    - Have an interest in children and young people's use of digital technology
    - Be familiar with safeguarding practices including the use of multi-agency procedures
    - Be able to receive e-safety concerns and ensure agreed procedures are followed
    - Have a commitment to multi-agency working

2. Each school / agency should have their own procedures for responding to e-safety concerns. This will include identifying whom needs to be informed, how decisions will be made and action to be taken. The process for referring concerns to outside agencies will be a central part of the policy.

3. Illegal material includes Images or material concerning the abuse and sexual exploitation of children. But this is not the only concern. Images and materials that incite racial hatred, terrorism, encourage or support crime and criminal activity are also illegal and of grave concern. Such activity must be reported to the local police and efforts must be made to secure and preserve evidence. Illegal activity on the Internet should also be reported to the Internet Watch Foundation (IWF). **The Police can be contacted on 0191 454 7555.**

4. Inappropriate material is anything that runs contrary to the school or agencies Acceptable Use Policy. This may be inappropriate images on a digital camera or mobile phone, the use of digital technology to bully or hurt others, sexual or violent images that whilst not illegal should not be accessed by the person concerned on school agency computers / mobile phones. If the person responsible is a member of staff accessing such material may have serious implications for the person's suitability to work with children.

5. Child protection concerns the deliberate abuse and neglect of children. This includes children abused for sexual and exploitative reasons no matter when and where the images/abuse originated. Locally only child protection social workers and police officers are empowered to investigate such concerns. There are also national organisations such as the Child Exploitation and On-line Protection Agency (CEOP), but the local police should inform CEOP if necessary. If the concern is likely to have significant impact on a child's health and development it must be referred to Children's Services or the Police Public Protection Unit. If in doubt contact them for advice and support. **Children's Referral and Assessment team**

is based Gateshead Civic Centre, Tel 0191 433 2525 or out of hours 0191 4770844. The Police Public Protection Unit is based at Whickham Police Station, Tel 0191 454 7555.

6. The Police are the agency responsible for responding to illegal activity. If digital equipment has been used it must be isolated and protected to preserve any evidence. Computers should **not** be closed down then switched off, but unplugged from the supply.

7. The individual agency / school policy should identify how issues that do not involve illegal activity or child protection matters are to be dealt with. This may be purely a decision for the individual school or agency but may require the input of other agencies or people. Make suggestions about what the steps may be

8. The Safeguarding Procedures are already in place and must be adhered to. Children's Services and the Police are the lead agencies and as such they must be informed about all child protection concerns. Other agencies **must not** undertake child protection investigations.

9. The Local Authority Designated Officer (LADO) is responsible for advising and supporting agencies when there has been an allegation against a member of staff concerning his or her suitability to work with children. Clearly, if a member of staff has engaged in illegal or inappropriate activity this may raise questions about this person's suitability. There is a formal process within the Safeguarding Procedures for responding to these situations and it must be adhered to. **The LADO is Joanna White within the Safeguarding Children Unit 0191 433 8011 or via e mail joannawhite@gateshead.gov.uk.**

10. It is important that each agency maintains a record of all e-safety incidents and concerns. This will enable the identification of patterns and themes that will help inform policy development. The information may be collated across Gateshead to help us understand how well we respond to and manage e-safety concerns. It will help us develop stronger polices, infrastructure and education to deal with e-safety in the future

APPENDIX E

FREQUENTLY ASKED QUESTIONS (FAQs)

This list of FAQs will hopefully provide some answers to your concerns and queries regarding e-safety. If you have further queries then they should initially be directed to the e-safety lead in your organisation (or your social worker, for foster carers) or the LADO.

Question 1
As a teacher, should I use my personal mobile phone to communicate with young people and their parents and should I use it to take photographs or videos?

No, do not use you personal mobile phone. Wherever possible workplace devices should be used to record images or communicate with parents and pupils. Organisations should also monitor the use of work mobile telephones to ensure compliance with the organisation's policy.

DfE offer guidance for staff on using mobile phones, and almost all schools have policies that prohibit their use. Employees should be given clear guidance on using their personal mobile phones by their employer, particularly regarding access to pupils numbers and giving pupils their number.

Question 2
Should I continue to use social networking sites, such as Facebook?

Yes, but bear in mind the DfE guidance that states "staff are strongly advised, in their own interests, to take steps to ensure that their personal data is not accessible to anybody who does not have permission to access it". Social networking is a way of life for most young people and many adults, however adults working with young people should review their use of social networking sites, as they take on professional responsibilities. Strong passwords should be used and security settings applied to control all access to your profile. Once information, such as photographs, is published on sites such as Facebook it is impossible to control and may be manipulated without your consent.

False social networking sites have also been set up by pupils and adults with malicious information about staff. Staff have also faced prosecution following inappropriate relationships with young people which have started with communications via Facebook and similar sites.

Remember- think before you post and ensure that your security settings only allow access to those who you wish to share your thoughts and photographs with, not unlimited and unrestricted access.

Question 3
Should I have my pupils as friends on instant messaging and social networking services?

No, pupils should not be added as friends. Communication between adult and children, by whatever method, should take place within clear and explicit professional boundaries. All professionals working with young people must understand what is appropriate. Professionals should not share any personal information with the young person, however innocent they may think it is. They should not request, or respond to, and personal information from the child or young person, other than what is appropriate to their professional role.

DfE have also produced clear guidance for adults working with young people on the use of social networking. This applies to anyone working with young people, not just teaching staff.

Question 4
I have a work laptop, what is my responsibility for the use of this at home?

There are no circumstances which justify adults possessing indecent images of children and all adults should ensure that they have absolute control of any work laptop allocated to them. There may be software controls in place to limit internet access in the workplace and often these do not exist when work laptops are used at home. Users must be aware that access to the wider internet may increase the risk of a virus attack or identity theft. There is an enormous variation as to what different adults find appropriate, funny, acceptable or offensive. Some adults may feel that it is acceptable to use a work laptop to view adult content outside of work hours. It is not; there is always a possibility that a child or young person may accidentally view this material. Many organisations now stipulate that the use of a work laptop for non-professional use is banned.

Question 5
What is "inappropriate material"?

It is important to differentiate between "inappropriate and illegal" and "inappropriate but legal". Adults working with young people must be aware that the former may lead to criminal investigation, prosecution, dismissal and barring. The latter can still lead to disciplinary action, even if there are no criminal proceedings.

Possessing or distributing indecent images of a young person is illegal. This may also include viewing such images online without saving them. Whether an image is "indecent" is ultimately down to a jury to decide and the police use a grading system for different types of indecent image. It is important to remember that children may be harmed or coerced into posing for such images and are therefore victims of child sexual abuse.

Material and images may also be considered inappropriate and/ or illegal if they inflict hatred, harm or harassment on the basis of race, religion, sexual orientation etc. It is an offence to send offensive or threatening messages with the purpose of causing the recipient distress or anxiety. There have also been instances where professionals have faced disciplinary action regarding disparaging marks relating to their pupils, colleagues or employer on social networking sites.

Workplace equipment should not be used to access adult pornography, dating websites, chat lines or adult materials. Adults working with children need to remember that they are role models and viewed as professionals by these young people. Whilst employees are private individuals, they also have a professional reputation and career to maintain.

Question 6
How can I use ICT to appropriately to communicate with young people?

Adults should always be circumspect in their communications with children and young people so as to avoid any possible misinterpretation of their motives or behaviour. Organisations should specifically discourage staff from using personal e-mail addresses or telephone numbers to communicate with young people.