

01

AN INTEGRATED APPROACH TO DEVELOPING SCHOOLS AS E-SAFE COMMUNITIES



PROMOTING E-SAFETY IN NORTHUMBERLAND SCHOOLS

e-safety training
policy & procedures
countywide accreditation & support
network controls
incident reporting



PROMOTING E-SAFETY IN NORTHUMBERLAND SCHOOLS

CONTENTS

<i>page 03</i>	Forewords <ul style="list-style-type: none">- Trevor Doughty - NSCB Chair- Northumbria Police
<i>page 04</i>	Introduction
<i>page 05</i>	National agenda
<i>page 05</i>	e-safe Northumberland schools
<i>page 06</i>	What's in the e-safety pack?
<i>page 07</i>	E-safe Northumberland schools
<i>page 08 - 09</i>	Overview - the L.A. integrated approach
<i>page 10</i>	Becoming an e-safe school
<i>page 10</i>	- Training
<i>page 10</i>	- Policies and procedures
<i>page 11</i>	- Network controls and monitoring tools
<i>page 12</i>	- Incident reporting and awareness
<i>page 13</i>	- NSCB reporting flowchart
<i>page 14</i>	- Countywide expectations, accreditation and support
<i>page 15</i>	Contacts and further information

FOREWORDS

I am delighted to launch this e-safety strategy pack on behalf of Northumberland Children's Services and The Northumberland Safeguarding Children Board.

New technologies offer many exciting opportunities for children and the staff that work with them and we must marry up these opportunities with the responsibilities we all have to ensure that children are safe and well protected at all times.

I hope you will take this opportunity to work with the Council and Safeguarding board, to ensure that children, staff, parents and the community have access to the best possible advice and resources to support e-safety.

Trevor Doughty
Executive Director of Northumberland Children's Services
and Chair of the Northumberland Safeguarding Children Board

Northumbria Police plays a crucial role in safeguarding young people and supporting partners to promote e-safety in schools and care settings, and will ensure that those who commit offences against vulnerable young people are brought to justice.

Technology continues to progress at a rapid rate and it is vital that all agencies continue to work together to develop, review and update their policies and practice in their response to e-safety issues, and promote safer practice and management of IT applications in schools and care settings.

Northumbria Police supports this integrated approach to e-safety which addresses strategic and practical issues to help young people use technology safely and promote e-safety guidance to adults working and caring for young people, to ensure the safe use of that technology.

Northumbria Police and partners work closely with the Child Exploitation Online Protection (CEOP) Team and this innovative e-safety programme of work can only enhance the 'Stay safe' safeguarding agenda.

Allan Brown
Superintendent, Northumberland Area Command, Public Protection Lead

This pack has been developed by the Northumberland e-learning and ICT support team to support schools in providing e-safety guidance to pupils, staff and the community. The team are keen to work with staff to further the e-safety agenda and we look forward to schools becoming accredited. Please contact John Devlin or myself should you require further information on any of the issues raised in the documents.

Richard Taylor
e-learning and ICT Adviser



INTRODUCTION

WHY IS E-SAFETY IMPORTANT?

INCREASINGLY PUPILS LIVE AND OPERATE IN A DIGITAL WORLD.

This world has steadily integrated with the classroom and, where activities involving the internet and communications technologies might have been a rarity a few years ago, they are now common place. Coupled with this, pupils have access to these technologies outside of school and potentially through a range of locations; home, libraries, free wifi sites and also through a variety of technologies ranging from mobile phones to portable games machines.

This regular use of technology within teaching and learning and outside of school, places risks on pupils, staff, governors, parents and the community. The risks for users are wide ranging - not just the dangers of viewing inappropriate content such as pornography, but racist, suicide and eating disorder sites, dangers from cyberbullying and contact from paedophiles.

The use of technology also brings many learning benefits and so risks need to be balanced up with the opportunities technology offers, and moderated by the careful and rigorous application of e-safety measures by schools. All users be they children or adults need a clear understanding of what the risks and dangers are, and how these can be safely managed.

Becta in 'Safeguarding children in a digital world comment:

'While it is clear that technology offers children unprecedented opportunities to learn, communicate, create, discover and be entertained in a virtual environment, there are some inherent risks. And whilst most children's confidence and competence in using the technologies is high, their knowledge and understanding of the risks may be low.'

It is this challenge we need to tackle in schools. To ensure that pupils are not just safe in school, but are prepared for the outside world and the use of these technologies in the home and community.

Similarly Tania Byron sees schools as an important source of information for parents and comments:

'Other risks are some times exacerbated because of the lack of experience and confidence parents have with using new technology and leaving them feeling unable to deal with any problems.'

All schools will have clear and effective procedures for promoting e-safety and raising awareness. They should already have a number of documents and procedures for tackling and promoting e-safety with pupils and staff. This document aims to draw together local and national resources, along with information on technical infrastructure provided through the Local Authority, into an integrated and accredited approach to e-safety.

Within the pack are a range of resources which together will enable schools to provide an accredited approach to tackling e-safety with pupils, staff, governors and the community.



Regular use of technology within teaching and learning and outside of school, places risks on pupils, staff, governors, parents and the community.



A NATIONAL AGENDA

Government has increasingly focused on tackling issues of online safety and a number of different organisations from the Child Exploitation and Online Protection agency to the Northumberland Safeguarding Children Board are now involved. Ofsted similarly are scrutinising procedures for safeguarding with increased rigour.

In her groundbreaking report, 'Safer Children in a Digital World', Tanya Byron sets out a number of recommendations that will establish a new culture of responsibility, where government, industry, parents and all those who work with children, can work together with the shared purpose of a safer online world. These include:

- That the Government takes this opportunity to encourage school leaders and teachers to focus on e-safety by identifying it as a national priority for continuous professional development (CPD) of teachers and the wider school workforce.
- That in all schools, action is taken at a whole school level to ensure that e-safety is maintained throughout the schools teaching, learning and other practices.
- 100% of schools should have acceptable use policies that are regularly reviewed, monitored and agreed with parents and students.
- That Ofsted take steps to hold schools to account and provide government with a detailed picture of schools performance on e-safety.

From September 2010, online safety will be a compulsory part of the curriculum for all children from age 5.

It is against this backdrop that the Local Authority and Northumberland Safeguarding Children Board are working together with other agencies to develop a range of policies and resources.

From September 2010, online safety will be a compulsory part of the curriculum for all children from age 5.

WHAT'S IN THE PACK?

OUR APPROACH HAS BEEN TO INTEGRATE THE RESOURCES, SUPPORT AND GUIDANCE AVAILABLE TO SCHOOLS INTO A SINGLE PACK OF MATERIALS PROVIDED WITH THIS DOCUMENT. THESE INCLUDE:

- Training materials for a variety of groups provided on cd-rom;
- Guidance and sample documents to help schools develop and implement policy and procedures also on cd-rom;
- Resources to help monitor and control network use and internet access, provided on the USB memory stick;
- Strong links with the Northumberland Safeguarding Children Board and the promotion of their materials and guidance, particularly the incident reporting flowchart;

And drawing this all together:

- A countywide accreditation scheme linked to the above resources and underpinned by support and guidance from the Local Authority e-learning and ICT support team.

The pack distributed to schools contains:

1. This document - 'An integrated approach to developing schools as e-safe communities' which forms the core of the pack and three other documents:
2. 'Safer practice with technology -Frequently Asked Questions';
3. 'The e-safety self assessment tool';
4. Guidance on 'Implementing network control and monitoring tools';
5. A USB data drive which contains the software for installing Policy Central Enterprise on school computers;
6. A cd-rom containing the training materials and additional resources such as exemplar policy documents and templates;
7. Information on registering your school for accreditation;
8. Information on training courses linked to the integrated approach, and covering e-safety and also network control software (PCE).



Support and guidance available to schools into a single pack of materials.



e-safety training

policy & procedures

network controls

incident reporting

countywide accreditation & support

E-SAFE NORTHUMBERLAND SCHOOLS

THERE ARE FIVE CLEAR STRANDS IN OUR APPROACH TO DEVELOPING E-SAFE NORTHUMBERLAND SCHOOLS.:

e-safety training

The first strand is to ensure that through training, pupils and adults have a clear understanding of the dangers and risks of use of technologies and also an understanding of what safe behaviour and practice is.

policy & procedures

Secondly, schools need to have up to date policies and procedures which are shared with all users and regularly updated and reviewed by staff, pupils, parents and governors.

network controls

To support schools, the Local Authority has provided network control and monitoring through Policy Central Enterprise, which enables schools to limit access to inappropriate material and monitor activity on their networks.

incident reporting

Schools can never guarantee that there will never be an e-safety incident and so our fourth strand is how to deal with a concern should one arise, what to do or not to do and who to contact.

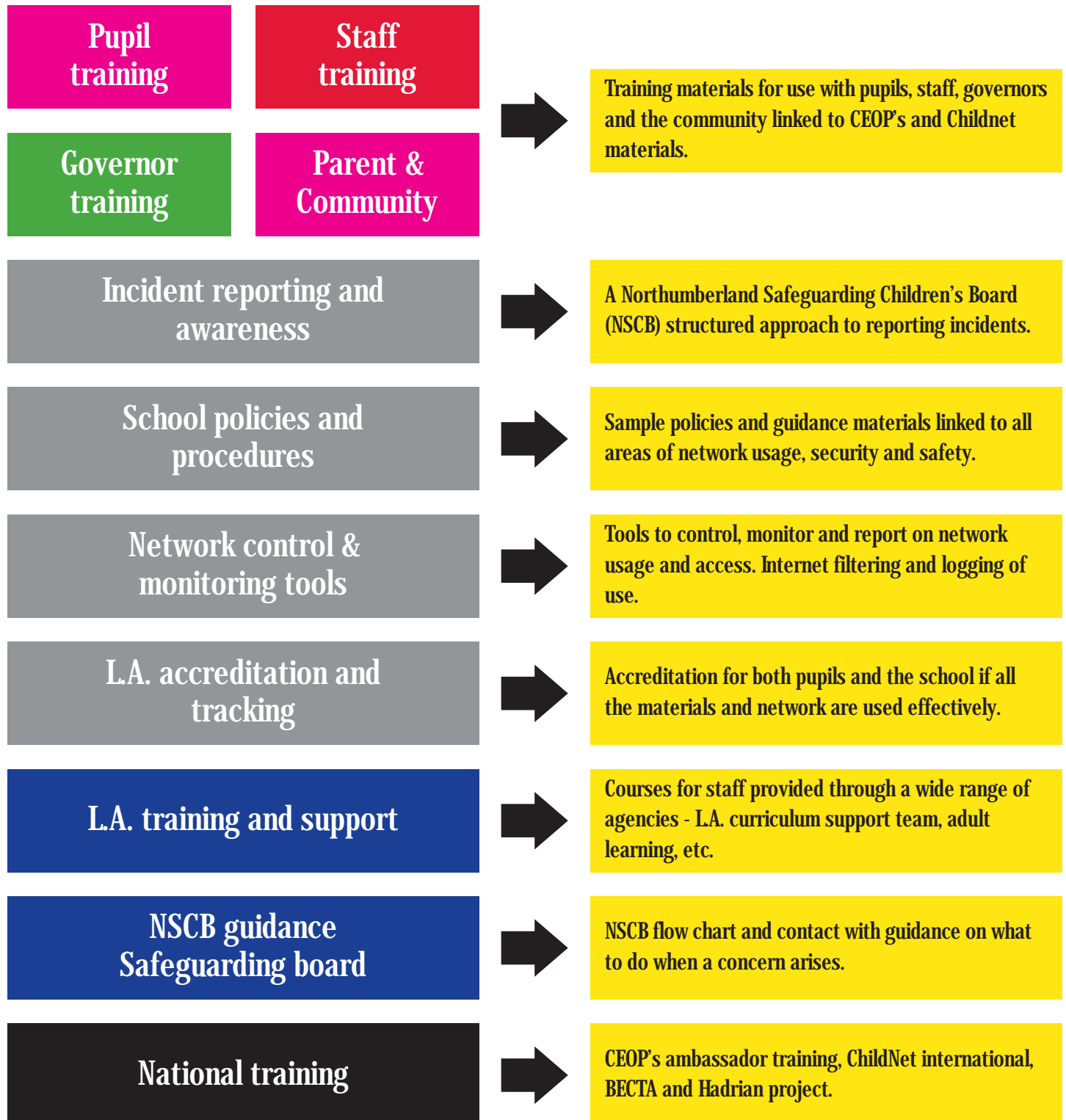
countywide accreditation & support

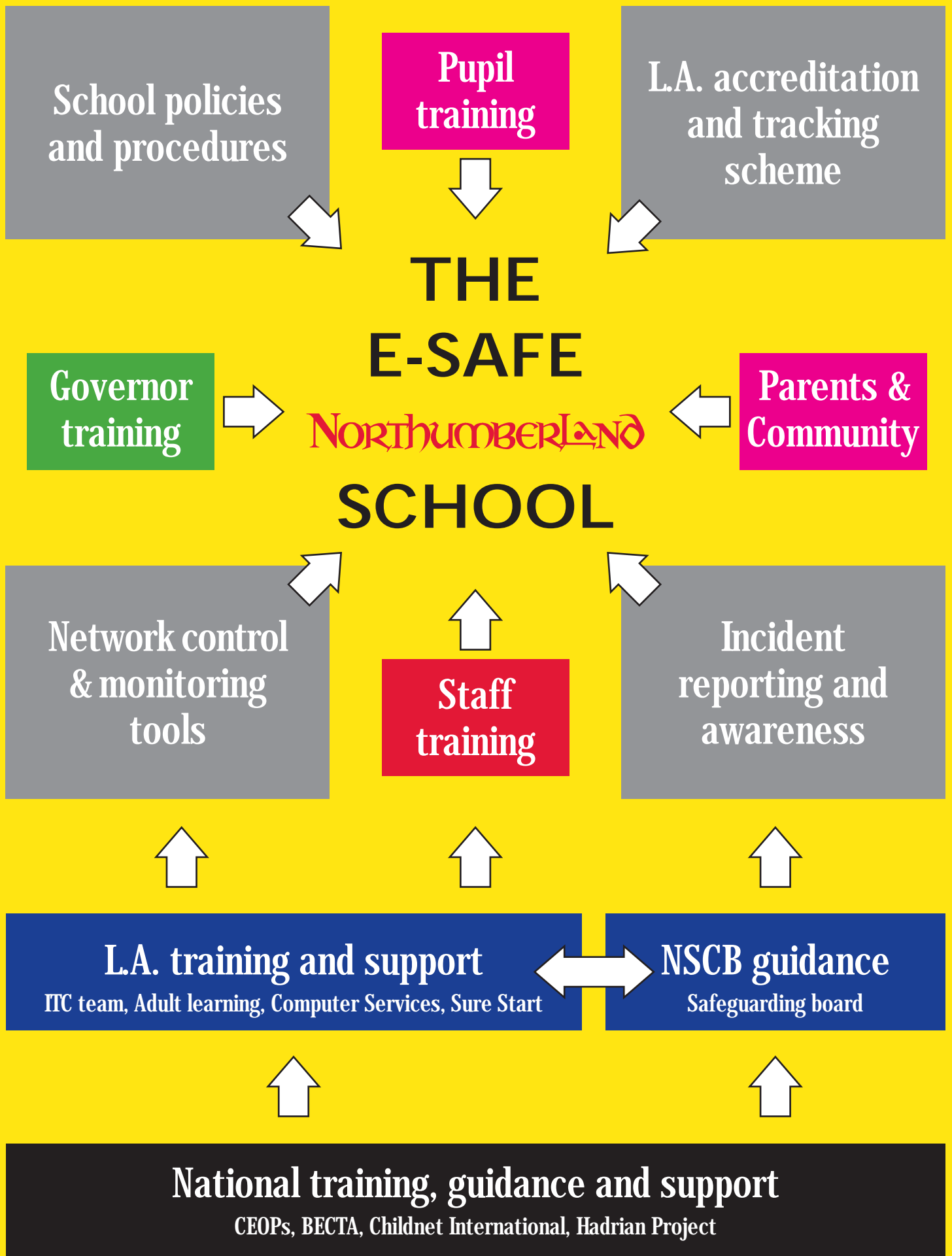
By implementing the first four elements, schools will be able to gain accreditation for both themselves and their pupils.

Overall, we aim to provide an integrated approach with materials for the training of different groups, monitoring access and also providing a system of accreditation for schools that have demonstrated systematic application of the resources.

There are five clear strands to our approach.

THE INTEGRATED APPROACH - OVERVIEW





BECOME AN E-SAFE SCHOOL

A

TRAINING - FOR PUPILS, STAFF, GOVERNORS, PARENTS AND THE COMMUNITY

This pack includes a cd-rom which contains training materials for pupils, staff, governors, parents and the community.

For schools with Primary aged pupils the approach is to use the Childnet International materials - Kara, Winston and the SMART Crew. All First, Special and Primary schools have been provided with these resources on the cd-rom included with this pack. The pack also includes a range of teacher education materials.

Linked to this, the Local Authority has also commissioned a number of Primary Literacy materials from Shoofly called 'The Pirates chest and other body parts'. This should enable schools to integrate the teaching of e-safety into a wider cross curricular context and so engage pupils more effectively.

For Secondary we are promoting the use of Child Exploitation and Online Protection agency (CEOP) materials including the 'Think U Know' educational programme, the Childnet International anti-cyberbullying DVD 'Let's fight it together' and other materials. These materials have also been sent to schools.

There are also a number of interactive KS2/3 materials on e-safety, produced by ROAR, on the Northumberland Teaching and Learning Environment (NorTLE).

The approach for staff, governors, parents and the community is based around using the Childnet International presentation, modified to reflect the Northumberland approach and make them more relevant for different audiences.



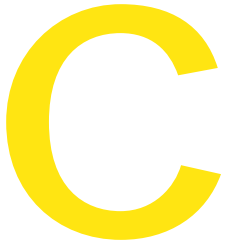
This pack includes a cd-rom which contains training materials for pupils, staff, governors, parents and the community.

B

REGULARLY REVIEWED SCHOOL POLICIES AND PROCEDURES

Schools are expected to have, as a minimum, Acceptable Use Policies for Staff and Pupils along with an e-safety policy. In addition Computer Services have produced a number of exemplar policies which schools need to consider in order to determine their appropriateness for their establishment and circumstances. Exemplar materials are available on the cdrom and website.





NETWORK CONTROLS AND MONITORING TOOLS

As part of their duty of care, services working with children and young people have a legal obligation to closely monitor access to their network and the Internet.

The Local Authority (L.A.) has now licensed Policy Central Enterprise (PCE) for all Northumberland schools. Policy Central Enterprise will provide schools with greater controls over their network and also enable them to monitor and track user activity more effectively.

It is being provided free to all schools and is included in the pack on the USB memory stick. PCE will also be adopted by other services such as Looked After Children, Adult Learning and other consultants who work in schools.

In the interests of online safety, the L.A. and Northumberland Safeguarding Children's Board will require that PCE be installed on all staff and pupil devices as part of the regulated provision of broadband services to schools.

If PCE is not implemented on all devices the L.A. may restrict Internet access to schools.

Training and guidance on the use of PCE and its implementation is available to all schools and the e-safety website contains up to date links.

PCE provides a range of features to ensure the online safety of pupils and staff, in particular identifying and preventing:

- Bullying and threatening behaviour
- Abusive comments or offensive attitudes
- Inadvertent exposure to inappropriate web sites (pornography, violence, suicide)
- Deliberate access to inappropriate web sites
- Un-moderated discussion forums and chat rooms

Schools need to implement a clear policy on how the information provided by PCE will be used to control and manage access to the network and identify infringements in the school.

It is important that schools also identify the appropriate member of staff who has access to PCE to monitor and report on activity and how this information is to be shared with staff, senior management and governors.



As part of their duty of care, services working with children and young people have a legal obligation to closely monitor access to their network and the Internet.

D

INCIDENT REPORTING AND AWARENESS

The Northumberland Safeguarding Children Board have produced the flowchart opposite which clearly identifies the procedures to be followed in the event of an e-safety concern being raised. Staff, pupils, governors and parents should all be aware of the correct procedure to follow should a concern be raised.

The following is taken from the letter sent to schools - G144-09 :

The Association of Directors of Children's Services (ADCS) have defined e-safety as:

'All fixed and mobile technologies that children and young people may encounter, now and in the future, which allow them access to content and communications that could raise issues or pose risks to their wellbeing and safety'

By virtue of its very broad nature it is very difficult to define the specific nature of an e-safety 'incident'. Depending on the presenting circumstances, different e-safety incidents will require different responses, and undoubtedly no two e-safety incidents will be exactly the same.

Some possible scenarios are illustrated in British Educational Communications and Technology Agency (BECTA) guidelines:

- accidental access to inappropriate material
- deliberate access to inappropriate material
- accidental access to illegal material
- deliberate access to illegal material
- inappropriate or illegal use of email
- inappropriate or illegal use of other technologies
- deliberate misuse of the network (for example, hacking or virus propagation)
- bullying or harassment using email or chat rooms

When a situation occurs, the expectation is that the child, young person or adult should report this incident immediately. If you have a concern, seek guidance using the NSCB flowchart. Refer to the website for up to date guidance.



When a situation occurs, the expectation is that the child, young person or adult should report this incident immediately.

A concern is raised



Please check the L.A. e-safety website for the latest version:

<http://ngfl.northumberland.gov.uk/e-safety>

Secure and preserve all evidence and hardware

Immediate response



If appropriate, seek advice and guidance from the Designated Officer for e-safety (Russell Pilling)



Inform the Senior Manager / Headteacher and designated e-safety officer and/or child protection staff. Make a written record of the concern

identify e-safety

Immediate response



NCC & SCHOOL NETWORKS

Contact the Information Security Officer for assistance in establishing the type of activity - 01670 533309

Contact the Local Authority Designated Officer, LADO: Andrea Carmichael to discuss the need for further action - 01670 533503

NON-NCC NETWORKS

Follow the relevant e-safety Incident Reporting and Child Protection procedures

Agree a strategy for dealing with the incident



Are there any Child Protection concerns?



No

Yes



Refer to the relevant information & Network Security Manager to consider further action



Internal Action

This might include

- Risk assessment
- Counselling
- Discipline
- Referral to other agencies
- Inform parents / carers if appropriate

Inform the Local Authority e.g. if a website needs blocking or child protection issues begin to emerge etc.

LADO will agree a strategy for intervention **Within 1 working day**

Possible referral to:

- Northumbria Police Specialist Investigation Unit
- Children's Services
- FACT Locality Office

Standard child protection procedures will then apply



Report to the designated officer for E-safety **Within 2 working days**



Consider whether the incident has procedural, training or security implications. Share the information appropriately

NORTHUMBERLAND

Northumberland County Council

E

COUNTYWIDE EXPECTATIONS, ACCREDITATION AND SUPPORT

The aim of the e-safe Northumberland school scheme is to draw together the range of necessary activities which help schools ensure that the use of Internet and other technologies is as safely managed as can be expected.

The Local Authority in promoting e-safety through the e-safe Northumberland school scheme has the following expectations:

1. All schools will have a designated person responsible for the management and coordination of e-safety in the school. This is not a technical role and this person should be on the teaching staff and have a significant post in the school.
2. The designated person for e-safety needs to have had either CEOPS or LA. e-safety training.
3. As a minimum the school should have current and annually reviewed policies, including:
 - An Acceptable Use Policy for Pupils,
 - An Acceptable Use Policy for Staff
 - A whole school e-safety policy.
4. Systems for Governor endorsement and review of policies.
5. Present an annual return to LA. indicating the above is complied with.

The above five expectations were made to schools in June 2008 as a requirement for the Local Authority to continue to provide Internet services to schools.

As part of our ongoing drive to support schools in safeguarding, and as part of the e-safe Northumberland school initiative, we will also expect schools from January 2010 to be working towards the following:

6. Adopt and disseminate to staff the NSCB flow chart on dealing with an e-safety incident.
7. Implement Policy Central Enterprise on all devices that are used to connect to the Internet by pupils and staff.
8. Provide training for pupils, staff, governors and the community.

Schools which fail to comply with items 1 - 8 may have their Internet access restricted by the Local Authority.

Schools can apply for accreditation through the Local Authority as part of the e-safe Northumberland school scheme.

The authority will offer a number of resources to support this:

1. Pupil certificates and e-safe Northumberland 'reward' - pen or similar with logo.
2. E-safe Northumberland school logo for use on school paperwork.
3. E-safe Northumberland school plaque to display in school.

Further information on registering and the above resources is available at:
<http://ngfl.northumberland.gov.uk/e-safety>



Schools which fail to comply with items 1 - 8 may have their Internet access restricted by the Local Authority.

Schools can apply for accreditation through the Local Authority as part of the e-safe Northumberland school scheme.

CONTACTS AND FURTHER INFORMATION

LOCAL

Russell Pilling - Head of safeguarding
russell.pilling@northumberland.gov.uk

Janet Ingham - Business manager for Northumberland Safeguarding Children's Board
Janet.ingham@northumberland.gov.uk

John Devlin - ICT Consultant
john.devlin@northumberland.gov.uk

Richard Taylor - ICT & e-learning Adviser
richard.taylor@northumberland.gov.uk

Chris Heane - Computer Services Network and Security manager
Chris.heane@northumberland.gov.uk

Andrea Carmichael - Local Authority Designated Officer
Andrea.carmichael@northumberland.gov.uk

Northumbria Police
www.northumbria.police.uk

NATIONAL

Child Exploitation and Online Protection
www.ceop.gov.uk

Childnet International
www.childnet.com

Becta
www.becta.org.uk



An integrated approach to developing schools as e-safe communities.

01

PROMOTING E-SAFETY IN NORTHUMBERLAND SCHOOLS

Learning and Development 0-19 Service
Learning, Skills and Family Support
People Directorate
Northumberland County Council
County Hall
Morpeth
NE61 2EF

Telephone: 01670 533000

<http://ngfl.northumberland.gov.uk/e-safety>