



Information on the use of Policy Central Enterprise in schools

Richard Taylor

ICT & e-learning Adviser

Informing users, getting procedures in place and understanding Policy Central's role within the wider integrated e-safety strategy in protecting staff and pupils

Northumberland County Council

**Draft for consultation please
respond to**

hepscott@northumberland.gov.uk

**with your name, school and
comments**

Guidance on implementing Policy Central Enterprise

Informing users, establishing procedures and understanding Policy Central's role, within the wider integrated e-safety strategy, in protecting staff and pupils.

Contents

| | |
|---|-----------|
| WHY IS E-SAFETY IMPORTANT? | 3 |
| A NATIONAL AGENDA | 3 |
| WHAT IS OUR APPROACH TO IMPROVING E-SAFETY FOR STAFF AND PUPILS ? | 4 |
| What is PCE? 4 | |
| HOW SHOULD IT BE USED? | 5 |
| WHAT IS A SIGNIFICANT INCIDENT? | 5 |
| WHAT IF I USE THE INTERNET FOR PERSONAL, NON SCHOOL RELATED ACTIVITIES? | 5 |
| WILL PCE KEEP TRACK OF MY PRIVATE AND PERSONAL USE OF THE INTERNET ? | 5 |
| WILL PCE CAPTURE MY PRIVATE EMAILS? | 6 |
| DOES PCE CAPTURE EVERYTHING THAT I DO? | 6 |
| WHAT IF I HAVE A CONFIDENTIAL SCHOOL MATTER TO DEAL WITH? | 6 |
| IS PCE THE SOLUTION TO INTERNET SAFETY IN SCHOOLS? | 7 |
| WHY THEN IS PCE NECESSARY? | 7 |
| SHOULD I BE INFORMED THAT PCE IS BEING USED? | 7 |
| SHOULD I HAVE A SAY IN HOW THIS IS BEING USED IN SCHOOL? | 7 |
| USING SCHOOL LAPTOPS AT HOME - WILL MY FAMILY BE LOGGED? | 8 |
| DON'T PANIC! - WE ALL STUMBLE ACROSS STUFF ! | 8 |
| WHOSE ROLE IN SCHOOL - WHO SHOULD HAVE ACCESS TO THE PCE CONSOLE? | 8 |
| AGREEING PROCEDURES, APPROACHES IN SCHOOL | 8 |
| · WHO SHOULD ACCESS THE CONSOLE? | 8 |
| · WHO SHOULD CREATE REPORTS? | 8 |
| · WHO FOLLOWS THROUGH IF AN INCIDENT OCCURS? | 8 |
| · WHICH DEVICES AND OPERATING SYSTEMS CAN PCE BE USED ON? | 9 |
| · WHAT ABOUT PRIVATE DEVICES, 6 TH FORM OR STAFF'S OWN? | 9 |
| · CAN STAFF USE THE INTERNET FOR NON SCHOOL RELATED ACTIVITIES | 9 |
| · DO STAFF NEED TO SIGN AN AUP? | 9 |
| INFORMING PUPILS, STAFF, PARENTS & GOVERNORS | 9 |
| HANDLING DATA – CONFIDENTIALITY | 10 |
| APPROACH TO MONITORING – TYPES OF REPORTS | 10 |
| WHY LOOK FOR THE SIGNIFICANT? – FALSE POSITIVES VS SIGNIFICANTLY HIGH CAPTURES | 10 |
| DEALING WITH INCIDENTS | 10 |
| RECORDING AND LOGS OF DEALING WITH INCIDENTS | 11 |
| CHECKLIST OF DO'S | 11 |
| TECHNICAL BITS – NETWORK SEEMS SLOW | 11 |
| USING PCE TO IMPROVE FILTERING | 11 |
| OPPORTUNITIES FOR PARENTS – CYBERSENTINEL | 12 |
| E-SAFETY WEBSITE | 12 |
| CONTACTS | 12 |

Why is e-safety important?

INCREASINGLY PUPILS AND STAFF 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.

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.

What is our approach to improving e-safety for staff and pupils ?

e-safety training

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

policy & procedures

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.

network controls

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.

incident reporting

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.

countywide accreditation & support

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.

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.

What is PCE?

Policy Central Enterprise (PCE) is the network monitoring software that Northumberland County Council is providing free to all schools.

PCE tracks the use of the computer, particularly when on the Internet and takes a 'screen grab' when an incident occurs which contravenes its rules list.

The rules lists are based around word banks covering areas such as profanity, race, sexual abuse and bullying. It also logs what websites are visited and enables schools to block websites causing concern.

How should it be used?

*PCE should be used by the senior management team of the school to monitor the network for **significant e-safety incidents**, where pupils and staff are put at risk.*

What is a significant incident?

A significant incident is one which could raise issues or pose risks to pupil or staff well being and safety.

PCE is provided for the express purpose of identifying e-safety incidents and providing protection to staff and pupils.

*It is **not** intended to monitor the trivia of Internet use, nor to enable leadership staff to implement over restrictive Acceptable Use Policies or to discipline colleagues for minor breaches of the AUP.*

What if I use the Internet for personal, non school related activities?

The use of the Internet and computers for personal purposes should be permitted.

Many schools encourage this, in that it helps teachers develop their own confidence and competence in using ICT.

Clearly the use has to be appropriate and at the appropriate time. Inappropriate times would include during lessons or when actively engaged in other duties. Inappropriate use would include deliberate access to illegal materials or misuse of the network (for example, hacking or virus propagation).

The corporate policy for ICT equipment similarly recognizes this, as long as use is at an appropriate time, i.e. lunchtimes and out of work hours.

Within the school, Governors should set acceptable use policies for staff use of curriculum machines, which recognizes this and reassures staff.

We strongly recommend that Governors adopt this flexible and reasonable approach and that staff are not discouraged from personal use of the internet, due to fears of falling foul of unreasonable or over restrictive AUP's.

Will PCE keep track of my private and personal use of the Internet ?

Confidentiality and privacy are real and understandable concerns for all staff. Ordinarily PCE should not capture private and personal material and is not set to track and log individuals' private email accounts.

However, because PCE captures are based on word lists, there is always the possibility that if an email contains a word on PCE's list, where it occurs a screen capture will take place.

If you are concerned about private and personal information being captured, the best advice is not to use school ICT equipment for viewing private and personal information.

If you are using the internet to deal with a confidential matter, for example a safeguarding incident, then it is better to use an Admin computer rather than a curriculum PC.

Will PCE capture my private emails?

If emails contain words on the banned list we cannot stop PCE from capturing them. Nor would we wish to, as there is evidence nationally is that email can be misused.

However, because of the unsophisticated nature of word lists, emails can be captured that are quite innocent. If staff want to guarantee their privacy, when using the internet for personal reasons, the best advice is to not to use work PC's to view personal emails.

At the end of the day the ICT resources are provided for teaching and learning purposes and if you want your actions to remain private, then the only way to ensure this is to use your own ICT equipment at home to access your private emails.

Because of the sensitivity relating to the use of PCE we have recommended that the use of the PCE console in a school be limited to two members of the senior management team with some child protection experience.

It is key that these staff keep the data on the PCE console private and respect the confidentiality of others.

We do not feel it appropriate for school network technicians to be given access to the console, since they are unlikely to have child protection training, nor are they normally represented at senior management team meetings where the PCE data needs to be reviewed.

School should regard the e-safety data on the PCE console in the same way they regard the achievement data on the Assessment data platform – purely as information to inform senior management decisions.

Does PCE capture everything that I do?

No, PCE does not capture everything that is taking place on a network or being done by an individual. Rather, it has a set of rules, which if an activity breaks them, a screen grab is instigated. The rules are based on word lists covering areas such as profanity, grooming, bullying, racism and violence.

PCE also has a set of filters which allow schools to block inappropriate websites. The software also provides a number of other useful tools, for example, it displays a schools Acceptable Use Policy (AUP) on start up, informs the user that the computer is being monitored and asks them to agree to this, logging their acceptance of the AUP. The software tracks the different websites visited in school and provides the SMT with useful data on the most popular sites in use.

What if I have a confidential school matter to deal with?

Confidential school matters such as child protection and medical issues are better being dealt with on school admin machines if staff want to avoid the chance that text in these documents or emails could initiate a screen capture (given that PCE is only on the curriculum network, which is shared with pupils) it is better that these types of issues are not dealt with on devices shared with pupils in any case.

Is PCE the solution to internet safety in schools?

No, Policy Central Enterprise (PCE), alone cannot guarantee that pupils and staff are safe. Rather it is part of a wider, integrated e-safety strategy promoting e-safety in Northumberland schools. The integrated e-safety strategy includes:

E-safety training materials for pupils, staff, governors and parents.

Policies and procedures to support the management of e-safety.

Information on what to do if an incident occurs.

Network monitoring tools – PCE.

Accreditation for pupils and schools.

Network monitoring using PCE can never be the total solution to e-safety and that is why training and awareness raising with all users are so important.

Our ultimate goal is to make pupils and staff safer, by making them aware of the risks and able to avoid unsafe situations, and not to turn schools into Internet Policemen.

Why then is PCE necessary?

Schools have a duty of care and a legal responsibility to protect pupils, staff and others who use their premises and resources. Recent national briefing has drawn to our attention that this includes a responsibility to be aware of what is taking place on the school network and take steps to protect staff and pupils from harm. PCE is necessary because it provides a series of tools which give senior management a clearer understanding of how the school network is being used, or misused.

Should I be informed that PCE is being used?

Yes, absolutely. All users, pupils, staff and visitors should be aware that PCE is in use in the school. On start up PCE displays the schools acceptable use policy and this should be updated to include a reference to PCE monitoring the network.

PCE cannot solve all the e-safety issues schools are experiencing, but perhaps equally important, is the deterrent effect that knowing the network is being more effectively managed brings. The real benefit of PCE is that it modifies pupil behaviour. Students are aware their actions on the network are being monitored and as a consequence avoid going to sites which they know are against the schools AUP.

By informing people that the network is monitored we take the first steps in ensuring that they are accountable for their behaviour.

Should I have a say in how this is being used in school?

Yes, consultation and involvement of staff on the e-safety process is vital. The use of PCE should be part of a school's Acceptable Use Policy and this should be collectively developed by staff. Pupils should also have an input into the AUP and be clear on what and why PCE is being used. All staff need to be trained in e-safety and be aware of the dangers and risks associated with the use of ICT and the Internet. PCE is a tool to help Senior managers in their legal responsibility and duty of care, but all of us share the responsibility of ensuring that pupils are as safe as possible.

Using school laptops at home - will my family be logged?

Whoever is using the PC will be logged. If you allow members of your family to use school equipment then their actions will be logged on the computer. Again if you, or your family are uncomfortable with being monitored by PCE in this way the best solution is to separate home and work life and only use the school computer for work purposes.

Don't Panic! - we all stumble across stuff !

You should not be worried if you accidentally come across inappropriate materials online.

Sadly, from time to time we will all come across inappropriate material on the internet or receive unsolicited emails with inappropriate content. The Local Authority and County Council does its best to minimize this through filtering, but no system can be 100% secure.

The purpose of PCE is not to track and follow every single incident and action on a computer but rather to look for trends and significant incidents. Where incidents occur our experience and guidance from the providers is that they are sustained, regular and a long series of screen captures rather than the occasional incident to which we are all prone to.

Whose role in school - who should have access to the PCE console?

We feel strongly that this is a role and responsibility for someone in the senior management team. Not least because it deals with child protection issues, but also because staff need to respect confidentiality and privacy. We have recommended that where possible 2 member of the SMT, in smaller schools probably the headteacher, should be trained in accessing PCE.

Agreeing procedures, approaches in school

There are some key policies and procedures about which a school needs to be clear on before using the PCE console.

AUP's need updating, staff need consulting and the management team needs to be clear on the following:

- **Who should access the console?**

We recommend access be restricted to two members of the SMT experience of safeguarding and child protection.

- **Who should create reports?**

Console users can create reports but we recommend you make use of the automated report system in order to cut down on work load and better focus on significant issues.

- **Who follows through if an incident occurs?**

This is a responsibility of the senior management team and the Northumberland Safeguarding Children Board has sent to all schools an incident reporting flowchart – school should make use of this to ensure correct procedures are followed.

- **Which devices and operating systems can PCE be used on?**

The PCE software is available for Windows XP, Vista & Windows 7 PCs and also for Linux and Mac and we recommend that all devices on the school network have the PCE software on them. If this is not the case then schools cannot be sure of the safety and security of the network for all users. Any single device which is allowed on without the PCE software is able to avoid the school's Acceptable Use Policy.

- **What about private devices, 6th form or staff's own?**

For PCE to be effective in a school it needs to be on all devices which make use of the curriculum network. Devices which use the Admin network are already monitored and do not require the installation of PCE.

One aspect that schools need to be clear about in their AUP and procedures is their approach to other devices brought in from outside the school. If a school allows some users to bring in devices, which do not have PCE installed, and use them on the network, it invalidates the entire PCE process.

The purpose of PCE is so that SMT know what is happening on their network and can be sure that inappropriate material is not brought in or the devices used inappropriately. If a device is allowed which is not covered then the SMT cannot be secure about network safety.

For outside users the privacy and confidentiality issues mentioned above will be a key concern.

- **Can staff use the Internet for non school related activities**

Yes, Council AUP guidelines indicate that this type of use is permitted, as long as it is outside of working hours and to appropriate websites. School's own AUP need to reflect this level of flexibility and senior leadership teams need to ensure that PCE is not used to enforce over restrictive AUP's.

- **Do staff need to sign an AUP?**

No, signing an AUP is not necessary, but it is an essential requirement that all schools have an AUP and that all users of the network are aware of it. Schools have many policies and procedures, health and safety, child protection etc, which are not signed by staff, but accepted as the agreed policies of the school, which members of the school community should adhere to.

It is important that the school AUP has been agreed with staff and ratified by the governing body.

AUP's need to be prominently displayed so that all users are familiar with them, this can be through posters, display in signing in books or distribution of printed copies. However, a better solution, which ensures that no one can use the network without agreeing to the AUP is to supplement these traditional approaches by having your AUP displayed on computers at sign on by PCE.

Informing pupils, staff, parents & governors

We feel it is fundamental that e-safety be seen as an issue, like any other aspect of safety, where every member of the school community, staff, pupils, governors, parents and visitors has a responsibility and role to play. For this reason the integrated e-safety packs contain resources for training all these groups.

It is vital that everyone is informed, involved and understands the reasons why PCE is being used and the benefits and security it brings.

We are all too aware of the incidents both locally and nationally which have given rise to the growing concerns about the use of the internet and the risks to young people. However we need to balance this with the benefits the Internet brings and recognize that PCE provides additional resources to protect both staff and pupils.

Handling data – confidentiality

It is essential that all data and information provided by the PCE console is treated confidentially. It is for this reason we have requested that schools identify members of the senior management team to training and ensure that the role of monitoring and reviewing network activity is carried out by the SMT.

Approach to monitoring – types of reports

Our intention with PCE is to improve the safety and security of staff and pupils when using the network. It is not to pry into the minutiae of every single network activity. Nor do we think it appropriate to increase busy staff's workloads by making them 'the Internet police'!

For this reason we are recommending that schools make use of the automated reporting features which can provide a weekly summary of activity on the network. Typically this is the top ten websites visited, the most prevalent screen captures.

The reason this is useful is that experience has shown that we need to look for '**the significant**' and that when an incident occurs it will be more than likely identifiable in these lists.

Schools have the ability to run, when necessary, more detailed reports and this has proved invaluable when Police are involved and the school needs to track back over its logs to identify what activity was taking place on a set day.

In our pilots, reviewing automated reports is a weekly SMT meeting task which takes less than five minutes.

The local authority is also piloting a managed service for schools, providing detailed reports on a half termly basis and also providing support on web filtering and managing groups of users.

Why look for the significant? – false positives vs significantly high captures

As mentioned above, all of us at times will come across things on the internet which will be captured by PCE. Staff should not be worried by this and these types of incidents are called false positives.

The reason we recommend looking for the significant is that, where 'real' incidents occur, the number of captures is many times higher than that of everyday users and can be quickly and easily identified through the automated reports.

Dealing with incidents

Where an incident occurs schools should respond by following the guidance issued by the Northumberland Safeguarding Children Board – a flowchart indicating how to proceed is available on the ngfl website - <http://ngfl.northumberland.gov.uk/e-safety>

Recording and logs of dealing with incidents

When an incident occurs it is important that the school keeps a clear record of what has and is taking place. The e-safety website has guidance and a recording log which can be used by schools.

Checklist of do's

1. Discuss at Senior Management Team and be clear on policy, practice and confidentiality.
2. Discuss with all staff and agree as part of your schools' wider e-safety and safeguarding policy.
3. Remind staff of the NSCB dealing with an incident flowchart.
4. Distribute to staff the NCC letter which provides more information about PCE and its role within the wider integrated e-safety strategy.
5. Keep the Local Authority posted, discuss any concerns or issues and help us work with you to develop our practice in this area.
6. Implement PCE on all computers
7. Move cautiously, act sensitively and respect confidentiality.
8. Look for the significant
9. Meet with the L.A. to review progress.

Technical bits – network seems slow

One or two schools have reported that following installation of PCE the network appears slower. This should not occur and in all instances we have found that the fault lies not with PCE but that it has highlighted problems with the configuration of the school Internet connection. By working with Computer Services we have been able to resolve this for schools.

If you have a concern, contact either the ICT team or Computer Services helpdesk.

Using PCE to improve filtering

PCE also has a comprehensive set of tools to help schools manage the filtering of websites. In the Autumn term we hope to develop this further with schools. Our wish would be to free up some websites blocked centrally and provide schools with the choice of whether to block them or not.

For example, Social networking sites are blocked at the moment. We would like to be able to open them up for schools, if they have given children and staff training on their safe use and how to avoid the risks.

See additional guidance on the use of social networking sites.

Opportunities for parents – Cybersentinel

The local authority has also negotiated to provide all homes in Northumberland with school age children with a domestic product, cybersentinel, which provides similar tools as PCE to the home. We are planning to roll this out from Autumn 2010 – for further information see the e-safety website.

E-safety website

Resources and further information is available at:

<http://ngfl.northumberland.gov.uk>

Contacts

Richard Taylor

ICT and e-learning adviser – Richard.taylor@northumberland.gov.uk

John Devlin

SEN and e-safety consultant – john.devlin@northumberland.gov.uk

Russell Pilling

Head of safeguarding – Russell.pilling@northumberland.gov.uk

Andrea Carmichael

Local Authority Designated Officer – andrea.Carmichael@northumberland.gov.uk