Hexham First School Online Safety Policy

1. RATIONALE

At Hexham First School, we believe that computing and the internet are valuable resources for both teachers and pupils and can help raise standards. Recognising the dangers and planning the use of suitable resources is vital to safeguard children in our school. Our aim is to promote safe use of ICT and online resources through the continual development of pupil, parent/carer, governors, support staff, and teacher awareness.

2. WHY IS ONLINE SAFETY IMPORTANT?

This policy document outlines how we educate children and parents/carers to use the internet safely. Children working online in school or at home should understand the risks they face and will be equipped with strategies to deal with issues as they arise.

Teachers, children, and parents/carers will receive information to highlight factors they should consider when using computing equipment and the internet. Pupils have access to technologies in various locations such as school, home, libraries, and through a wide variety of technologies ranging from mobile phones to portable games consoles.

At Hexham First School, we develop an awareness of Online Safety through the use of our Acceptable Use Policy (AUP), which is sent home for parents/carers and children to sign.

3. SCHOOL STAFF

Due to continual developments in computing, planning and practice need to be assessed and changed to suit the needs of the children in our school. At Hexham First School, it is essential that the staff are briefed on procedures that will allow them to deal with discussions about children's internet use and online presence.

Staff receive the necessary training and advice to combat problems children in their class may face. Advice and training may be obtained from outside agencies/advisors such as the child protection officer. Documents such as:

- Hexham First School Online Safety Policy 2025
- Teaching Online Safety in Schools - DFE 2022
- Keeping Children Safe in Education - DFE 2024
- Cyberbullying: Advice for Headteachers and School Staff

- Promoting online safety in Northumberland Schools

To continue developing strategies to enhance online safety in our school, the Online Safety Team regularly attends online training and updates. Key information will be fed back to the staff through briefing notes, policy documents, and staff development sessions.

The school ethos encourages trust between staff, pupils, and parents/carers. As teachers, it is part of our role to safeguard children in our care and educate them about how to safely use ICT equipment and the internet both in and out of school.

Each academic year, all staff members are required to sign an Acceptable Use Policy. In signing, staff members accept that the school can monitor network and internet use to help ensure staff and pupil safety.

On entry to the school, supply teachers, trainees, external agencies conducting work, parent helpers, and all adults on site are asked to read and sign an AUP Policy.

At Hexham First School, an effective approach to online safety empowers our school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable but can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate, or harmful material;
- Contact: being subjected to harmful online interaction with other users; and
- Conduct: personal online behaviour that increases the likelihood of, or causes harm.

Staff will be briefed on procedures that define how inappropriate or illegal ICT use is reported to the senior management. The Leadership team will follow set procedures and investigate incidents with care and attention. Staff will be briefed on the dangers of mismanagement of ICT, for example, the potential for children to view inappropriate images if a search engine is used during a lesson without prior planning.

Staff are given a work Gmail account, which is supplied by Northumberland County Council. Staff must use ‘2 factor verification’ when logging into email accounts on any device.

Communication is vital in a school and is key to the smooth running of Hexham First School. Staff members may be required to use school telephones, which is essential to the safeguarding of children. The use of personal mobile phones is prohibited during teaching time when phones should be switched off. Personal mobiles must not be used to store images of children.

Pupils who need to bring mobile phones to school for safety reasons when travelling to and from school must hand the phone into the Main Office. The pupil’s phone is stored here for the duration of the day, and an agreement must be signed between the parent

and school. Phones must be switched off before they are handed in, and children are to sign them in and out of the secure storage with office staff. No teaching staff are permitted to store pupil phones within the classroom.

4. ROUTES TO ONLINE SAFETY

Open access to the internet has become an integral part of children's lives. A growing danger is presented by the ease of uploading material to the internet. We are aware of primary pupils using social media at home. Social networking sites allow children to set up an account and create a web page in minutes.

Online safety will be introduced to children through a whole school approach at the beginning of every academic year. Through planned lessons, children will develop a better insight into the meaning of 'Online Safety' within the context of school and home. A new curriculum map for e-safety has been developed to ensure that e-safety is taught across the year and not in isolation. A series of web-links are sent out to parents via the school bulletin to update them with support and advice.

Staff must be prepared to tackle online safety issues as they arise throughout the school year, especially in Key Stage 2. This will mean adapting curriculum planning to e-safety situations as they arise. Any incidents should be passed on to the DSL and Computing Lead.

Raising awareness among children and young people of the risks associated with the internet and apps, whilst not wishing to alarm anyone, is a responsibility for all members of staff. Staff will be asked to review and refine their practises to ensure pupils are safe.

Through online safety teaching, we will educate children about the dangers of accessing sites through links sent to them, in-app extras, and online gaming. We will highlight the need to seek advice from teachers or family members. Pupils will be told not to upload photographs or videos of themselves or other pupils. They must not publish personal information, such as their address or contact details.

5. PARENTAL INVOLVEMENT

Working alongside parents/carers is vital when promoting online safety, as children can spend a lot of time using ICT in their homes, such as internet browsing, chat rooms, messenger facilities, and games consoles. Providing parents/carers with the appropriate information regarding safeguarding their children is essential. Key areas to be focused on will be:

- Mobile phones
- Selfies
- Internet grooming
- Gaming websites or consoles that can be attached to the Internet
- Social networking sites
- Cyberbullying
- Chat forums or blogs

Parents/carers will be made aware of how they can report incidents using the ‘Report Abuse’ facility on the ‘Think You Know’ homepage. Parents will be provided with information about how we intend to promote online safety in school and the rules/contract we will implement.

6. IDENTIFYING VULNERABLE GROUPS

The majority of pupils have access to mobile devices. The use of smart devices and handheld games consoles outside school is commonplace. The most ICT-capable may be the most vulnerable. Children who interact poorly socially may be more at risk from inappropriate online contact. As part of our home-school agreement, a copy of the School’s Online Safety Policy will be sent to parents and governors.

7. USING THE INTERNET TO SUPPORT LEARNING

Websites and apps are essential to teaching. Staff members are encouraged to use safe, purposeful sites and apps that are beneficial to learners. Through the use of the ‘Northumberland Grid for Learning Homepage’ and the Online Learning Platform ‘School 360’, website are recommended that contain suitable content to assist teaching and learning. We encourage children to use the learning platform as a means of searching safely by using the online resources. We recognise that there is always an element of risk: even an innocent search can occasionally turn up links to adult content or violent imagery.

For the youngest pupils, the greatest risk is through inadvertent access. Fast WiFi speeds mean that inappropriate images can appear almost instantaneously. Children can innocently follow a series of links to undesirable content.

In order to combat this issue, a procedure has been agreed by staff on how to handle the situation with pupils. Teachers will be advised to:

- Tell children to minimise the screen immediately.
- Do not navigate away from the screen.
- Talk to children about what has happened and reassure them they are not in trouble.
- Later investigate the history of the sites visited to get details of the inappropriate site and how the child got there.
- Report the incident using the appropriate form.

In light of potential problems when accessing Internet sites or search engines, pupils are not permitted to use the internet or an iPad in school unless they are supervised by an adult at all times.

8. SEARCH ENGINES

To combat problematic sites, children will be supervised when using internet-wide search engines. Staff will research websites and provide children with a link to click on. Children do not have access to the App Store on iPads to ensure they do not search for inappropriate apps. When accessing the internet on the iPads, children need to log into Fortinet. This tracks the websites being used.

9. CURRICULUM PLANNING

Good planning and preparation are critical in ensuring a safe starting point for online safety teaching. Online safety is planned as part of the computing curriculum. Using the computing curriculum map, year groups plan for age-appropriate online safety themes. Online safety is the first computing unit of work for all year groups. Teachers also teach online safety ‘incidentally’ when issues and questions arise throughout the academic year.

10. EMAIL

For external email linked to School 360, access has been switched off and children do not have access. Staff should not give out their own personal emails to pupils.

11. ONLINE FOR PUPILS WITH ADDITIONAL NEEDS

At Hexham First School, we are aware that some children may not necessarily understand the term “safety.” Children will take part in Key Stage assemblies where safety will be addressed through multimedia presentations provided by Project Evolve and the ‘Think U Know’ site, which provides suitable material for varying age ranges.

As part of the computing curriculum, teachers will be required to teach children safety rules in a way that does not frighten them and which gives them confidence to know what to do in certain situations. When children progress from Key Stage One to Key Stage Two, rules and guidelines are adjusted and changed in accordance with their age.

Children need to learn how to apply strategies that will help them to avoid certain “risks” such that they need to plan ahead. Visual aids will be displayed in the classrooms and areas where children come into contact with ICT to promote safety.

There are certain aspects of the above that are particularly challenging for pupils with additional needs and children who we may consider to be vulnerable in this learning context. Children will clearly have individual needs that will present different issues when teaching online safety, but some common difficulties may be:

- They may be still developing their social understanding of safety and so may relate better to strategies used with younger children.
- They are likely to find it hard to apply the same rules in different situations.

- Most safety principles rely on children being able to explain what happened or to ask for help.
- Some children may have poor recall and difficulties with learning through experience.

Adults working with children who are at more risk will be given appropriate resources to promote safety, including visual aids, websites, and advice on how to develop children's awareness of how to use the Internet safely. Adults need to plan group interactions carefully when raising awareness of internet safety.

The Designated Safeguarding Lead (DSL) is Justine Overton. In her absence,Bernadette Noon is also a trained DSL lead if Justine Overton is not available.

12. RESPONSE TO AN INCIDENT OF CONCERN

Web-based technology provides children and young people with the opportunity to broaden their learning experience and develop creativity in and out of school. We recognise the importance of considering the risks associated with technology our children come into contact with.

At Hexham First School, we develop the skills that children and young people need when communicating and using these web-based technologies properly, while keeping safe and secure, and acting with respect for other users. Links to Childline are visible on the Northumberland Grid for Learning homepage.

Our school website is populated with resources to aid children, parents, and teachers when reporting safety concerns.

These risks to online safety are, of course, caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are our first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to occasional extremely concerning incidents that may involve Child Protection Officers or the Police.

This section will provide guidance to help staff determine what action they can take within the school and when to hand the issue over to the school-based Child Protection Coordinator, the Online Safety Officer, or the Police Liaison Officer.

What Does Electronic Communication Include?

- Internet collaboration tools: social networking sites and blogs
- Internet Research: websites, search engines, and web browsers
- Mobile Phones and personal digital assistants (PDAs)
- Internet communications: e-Mail and instant messaging (IM)
- Webcams and videoconferencing

What Are The Risks?

- Receiving inappropriate content
- Publishing inappropriate content
- Predation and grooming
- Online gambling
- Requests for personal information
- Misuse of computer systems
- Viewing ‘incitement’ sites
- Publishing personal information/images
- Bullying and threats
- Hacking and security breaches
- Identity theft

How Do We Respond?

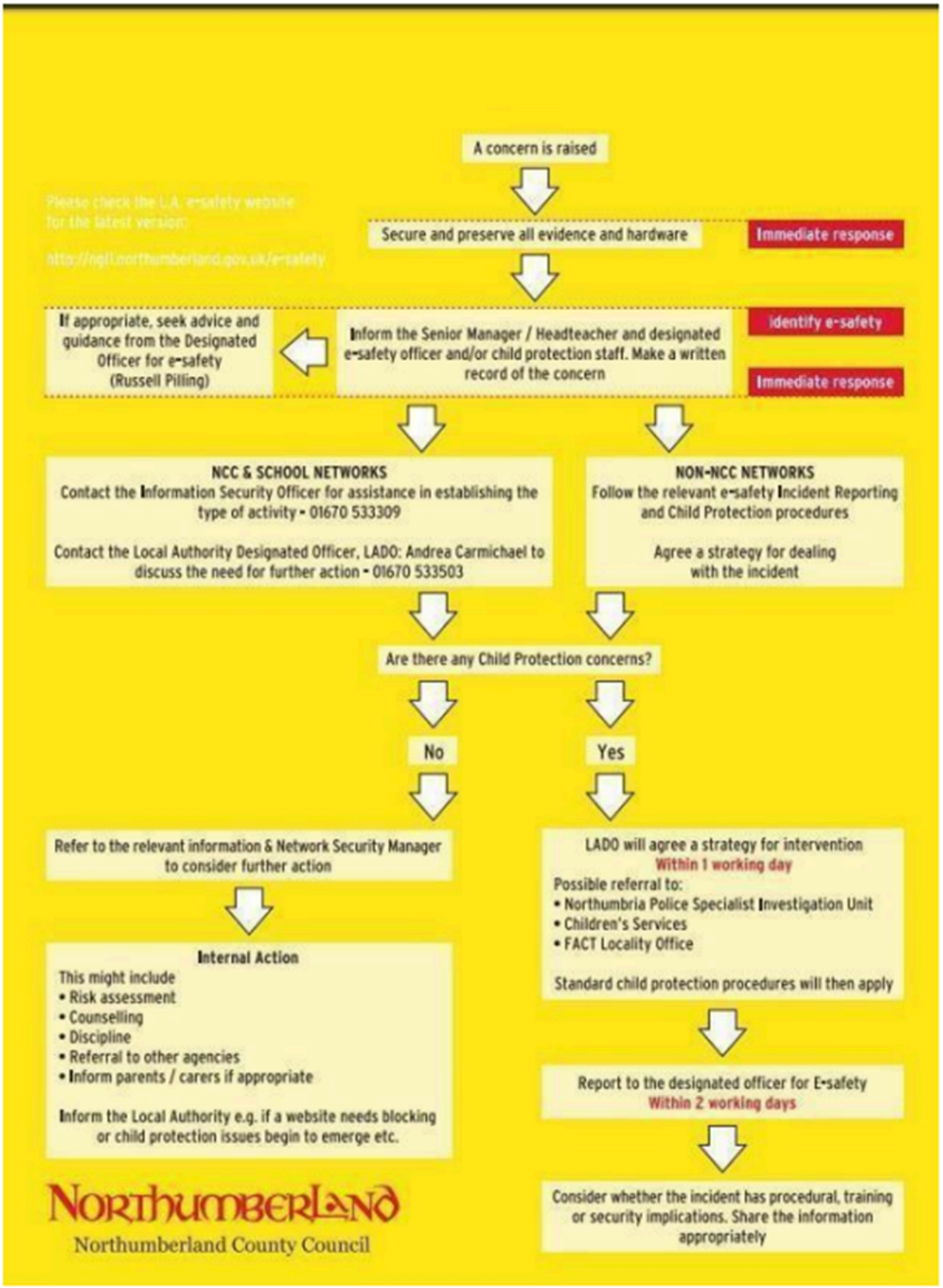
The Northumberland Safeguarding Children Board (NSBC) has provided guidance on how incidents should be reported, providing a flowchart of guidance. The expected response will be to report incidents to the Designated Senior Person for Child Protection/Online Safety representative in the school. The Child Protection representative will then refer details of the incident to the lead agencies involved in safeguarding children.

The flowchart on this page is the approach used to investigate an incident of concern. Staff will be made aware of supporting documents to assist schools when responding to incidents. Possible scenarios include:

- Accidental/deliberate access to inappropriate material
- Accidental/deliberate access to illegal materials
- Inappropriate/appropriate use of email
- Deliberate misuse of the network
- Bullying or harassment through email/chat facilities.

Please refer to the Children's Safeguards Service website:

- CEOP Annual Review – https://ceop.police.uk/Documents/ceopdocs/AnnualReviewCentrePlan2013_(0714).pdf
- Childline – http://ngfl.northumberland.gov.uk/website/childline/227742
- Online Safety link - http://ngfl.northumberland.gov.uk/website/online_safety/110036
- Reporting procedure - http://ngfl.northumberland.gov.uk/website/esafety_incident_reporting/221677
- Incident flowchart - http://www.northumberland.gov.uk/WAMDocuments/077B7977-71D9-42C9-A6D52974CAF7BF95_2_0.pdf?nccredirect=1


A concern is raised
Please check the LA 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

REPORTING AN E-SAFETY INCIDENT - ALL SETTINGS

SETTING

IMMEDIATE ACTION

A CONCERN IS RAISED

Seek advice from the designated person for e-safety and/or Local Authority

Secure and preserve all evidence and hardware in the interim

This might mean isolating a machine and making sure it's not used, do not switch off the device as this might lose important evidence

Inform your senior manager and child protection staff

Make a written record of the concern and your actions

LOCAL AUTHORITY

NCC & School networks

Contact JD/RT to discuss incident and plan of action
john.devlin@northumberland.gov.uk /
richard.taylor@northumberland.gov.uk

JD/RT to coordinate the investigation of the incident

Liaise with the e-safety lead in setting, Info Services security team, legal service and police as appropriate

Are there any Child Protection concerns?

No

Yes Contact LADO

LADO will agree a strategy for intervention

Within 1 working day

Possible referral to:

- Northumbria Police Specialist Investigation Unit
- CS e-safety SLA Team
- FACT Locality Office

JD/RT organise internal investigation, liaise with setting and report

this might include: PCE analysis, forensic examination and securing of equipment, liaison with Info Services security team, liaise with legal service and police

Non-NCC Networks

Follow your relevant e-safety Incident Reporting and Child Protection procedures and agree a strategy for dealing with the incident.

For information and advice, contact the Local Authority Designated Officer (LADO)

Chris.O'Reilly@northumberland.gcsx.gov.uk

ALL PARTIES

Report to Designated Officer for e-safety, School, Head of Service

REVIEW by LA and School:

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

12.

Information Security Event
Report Compiled by
Title
Date
Managed by
NATURE OF EVENT
Violation, weakness, other
Date of Report Time of Report
Reported to
Person making the report
Status Individuals, groups, systems involved
Incident reference number
Events witnessed by
Closure action

13. INFORMATION SYSTEMS INTEGRITY AND SECURITY

We have a responsibility to ensure that our capital investment in Computing is protected and secured. Changes or modifications to the hardware, network wiring, or software configurations will be completed by designated support personnel. All modifications will be logged.

At Hexham First School, the administration network has access to the Northumberland County Council Intranet, which is not accessible externally. A firewall is in place and prevents access from external sites to the curriculum network. Administration computers are protected via an Internet Service Provider (ISA) Server at our school and other ISA servers at County Hall. Administration sites are filtered by a product called Webmarshal.

The curriculum sites are filtered at the ISP level using an Equiinet Box and then again using the software Fortinet. Fortinet sessions are created for individual users based on

their network accounts. Fortinet provides global filtering for schools in Northumberland. Any sites deemed inappropriate that slip through the filtering system should be reported to the IT Help Desk at Northumberland County Council.

Antivirus software is installed throughout our school and is regularly updated. Staff desktops, staff laptops, and children's desktops are protected by online safety antivirus software provided by the NCC (Symantec). Additional software has been installed on staff desktops to scan USB memory sticks for possible threats of infection and remove them.

13.1 SENSO – Web Monitoring

SENSO runs in the background of all desktops in school. It enables a key logging system, and a weekly report is generated. This report can be seen by the designated personnel Justine Overton, Bernadette Noon, and other relevant staff. Any queries about the report are followed up, and staff are involved when necessary.

Our school server has a series of network shares that allow access to particular users. An outline of the school server can be found in the Computing File. The network shares were set up to provide shared access for teaching staff but to restrict the access of supply staff and children to common network shares.

14. DISASTER RECOVERY SYSTEM

In case of drive or network share failure, the curriculum server itself utilises RAID to share duplicate instances of data across multiple drives in real-time. The curriculum server has shadow (previous) versions enabled in case data is lost, deleted, or corrupted. The curriculum server backs up a Windows Server backup to an onsite NAS storage box, situated in the HUB

The curriculum server remotely backs up (encrypted) data to a secure offsite backup site in Newcastle each night. We have several backup methodologies in place at Hexham First School; these are outlined below. No data or hardware is kept on-site as a backup. We have a curriculum server.

In case of drive or network share failure, the curriculum server itself utilises RAID to share duplicate instances of data across multiple drives in real-time. The curriculum server has shadow (previous) versions enabled in case data is lost, deleted, or corrupted. The curriculum server backs up a Windows Server backup to an onsite NAS storage box, situated in the Hub. The curriculum server remotely backs up (encrypted) data to a secure offsite backup site in Newcastle each night.

15. MAINTENANCE

Part of our investment into Computing has been to pay for the local authority computing SLA , a technician from an IT company called 'Omnicom'. A technician visits the site monthly. The technician completes numerous jobs including antivirus checks, defragging

systems, installing software, and generally making systems more user-friendly and efficient.

16. USEFUL WEBSITES

- Reporting procedure: http://ngfl.northumberland.gov.uk/esafe/incident_reporting.html
- Incident flowchart: http://ngfl.northumberland.gov.uk/esafety/documents/NEWFLOWCHARTMAY2012.pdf
- CEOP Key principles of effective prevention: www.thinkuknow.co.uk/Documents/PSHE%20Association%20report%20to%20CEOP%20April%202016.pdf