Forest Federation

E-Safety Policy

2015/16

Contents

Policy Statement

ICT and the internet have become integral to teaching and learning within schools; providing children, young people and staff with opportunities to improve understanding, access online resources and communicate with the world at the touch of a button. At present, the internet based technologies used extensively by young people in both home and school environments include:

- Websites
- Social Media
- Mobile phones
- Tablets
- Online gaming
- Learning Platforms and Virtual Learning Environments
- Video broadcasting
- Blogs and Wikis
- Email, Instant Messaging and Chat Rooms

Why do school or organisations need an e-safety policy?

Schools and other settings must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. Organisations must be aware that children and staff cannot be completely prevented from risks using the internet. In accordance to Ofsted requirements young people need to be empowered and educated to make healthy and responsible decisions when using the internet in particular social media. E-Safety like safeguarding must be a whole school or organisation approach and all staff must take appropriate measures to keep young people and themselves safe using the internet and social media. Members of staff also need to be aware and informed about how to manage their own professional reputation online and demonstrate online behaviours that are in line with their job role. Due to this schools and organisations should develop a holistic approach in writing and developing an effective e-safety policy that must embed safe practice for students and teachers/practitonaners.

Scope of the policy

This policy applies to all staff, pupils, governors, visitors and contractors accessing the internet or using technological devices on the school premises and outside. This must include staff or pupil personal devices such as mobile phones and tablets which have been brought onto school grounds. The policy must also take into consideration devices the school has issued members of staff and pupils to use on and off site.

Who will write and review the policy?

The e-safety policy informs many different school or organisation polices such as the ICT Policy, Child Protection Policy, Safeguarding Policy, Anti-Bullying and school development plan and for the policy to be effective it should relate to other policies such as behaviour, PSHE and Citizenship. A solid policy allows an effective method to review good practice. The more people involved in creating the policy the more effective the policy will be you may want to consider involving pupils, parents and governors.

As per Ofsted requirements it is recommended a designated individual within the school or setting takes responsibility for e-safety. The designated person will need to have been e-safety trained and this can be provided through the Northamptonshire County Council e-safety officer.

Policy Decisions

The school should allocate internet access to staff and pupils on the basis of their educational need. It should be made very clear who can access what within the school. At primary level pupil usage should be fully supervised however filtering at home and school is only a small safeguarding intervention. Young people need to be able to make healthy decisions online in school and online at home irrespective of the device. Students at primary level must be aware that the internet is filtered and the consequences of accessing inappropriate materials. It is advised students sign an acceptable use policy at the start of the academic year. Also encourage parents to sign an acceptable use policy on the internet on behalf of their son or daughter encouraging safer internet use and endorsing the schools boundaries. It is also worth considering that some young people are very vulnerable and parents or carers may not want their son or daughter to have unrestricted access to the internet. There may also be some overlap in the schools behaviour policy. The above may be best coordinated when pupils home details are sent home and details are checked as part of the home school agreement.

For more information on acceptable use policies please follow:

http://www.swgfl.org.uk/products-services/Online-Safety-Services/E-Safety-Resources/creating-an-esafety-policy

Leading standards

- The school will maintain an up to do date log of all pupils who are granted access to the schools internet.
- All staff will read and sign an acceptable use policy before using any equipment and this is reviewed every 12 months.
- Parents and pupils are also asked to sign an acceptable use policy. As good practice parents can also counter sign the students acceptable use policy.
- All visitors to the school or organisation that require computer and/or internet access are to read and sign and acceptable use policy.
- Parents are informed that pupils will be provided with supervised internet access and will be asked to read and sign an acceptable use policy.
- When considering access to vulnerable members of the school, such as children with special educational needs, the school will make decisions based on the needs and understating of the pupil/s.

Suggestions for secondary and primary

- At key stage 1 pupil's access to the internet could be adult demonstration with occasional directly supervised access to specific and approved materials online.
- At key stage 2 pupils could be supervised. Pupils will use age-appropriate search engines, online tools and online activities will be teacher directed where necessary.

How will the policy be discussed with staff?

All staff need to feel confident in the use of new technologies and policies will only be effective if the whole school community buy into its values and methods. It's highly recommended that any polices or e-safety guidance are reviewed every 6 months due to the ever changing nature of technology. Staff should also be given opportunities to discuss issues and develop appropriate teaching methods. It wouldn't be suitable for instance for a cover teacher to deliver an e-safety class/sessions without reasonable preparation. If a member of staff is concerned about any aspect their ICT use of the internet on or off site they should discuss their concerns immediately with their line manager.

An area that needs specific attention are where staff is provided with internet enabled devices funded by the school or organisation and are accessed outside of the school network. Schools must make it very clear about the safe and appropriate use of the equipment provided by the school and have rules in place if the equipment is going to be used by third parties. Staff must be aware of their responsibilities to maintain confidentiality of school information.

The use of ICT is very widespread so it's essential that administrators, supervisors, caretakers, parents, teaching assistants, volunteers and governors are included in e-safety awareness training. Induction of new staff must included discussions around the e-safety policy and the new member of staff is to sign and date a copy of the policy and return it to the appropriate person.

Areas of consideration

- The e-safety policy will be distributed and discussed with all members of staff.
- Also the policy will be easily accessible for the school community.
- To protect the school community the school will implement acceptable use polices.
- Staff, students and parents will me made aware that internet access is monitored and can be traced back to an individuals account.
- Up to date and appropriate training for staff in e-safety is provided at least every 12 months this can be sought through Northamptonshire County Council's e-safety advisor.
- Members of staff who manage filtering systems or monitor ICT use will have clear procedures and will be appropriately supervised by SLT for reporting issues.
- The school will make use and cascade useful e-safety resources out to the school community.
- As above staff are fully aware of the importance of their online conduct in and out of school. Civil, legal, or disciplinary action could be taken if they are found to bring the profession or institution into disrepute.

How will risks be assessed?

E-Safety is an ever growing area and is always developing as things are constantly changing it is extremely difficult to safeguard against every situation. The school or organisation will need to address the fact that it is not possible to completely remove all risks that pupils and staff might access unsuitable material via a system in a school. It is always wise to include a disclaimer because as mentioned above e-safety is a difficult area to safeguard.

Areas of consideration

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the internet and social media being so vast it is not possible to guarantee that access to undesirable material will never occur via a school computer or Wi-Fi. The school cannot accept liability for the material accessed, or any consequences resulting from the internet use.

- The school should be auditing ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate. A full e-safety audit can be found on the County Councils website under e-safety.

- The use of any computer system without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches should be reported to Northamptonshire Police.

- Methods to identify, assess and minimise risk will be reviewed regularly.

- Logging reported incidents

- Action taken on incidents that occur such as cyberbullying

- Internal monitoring or data for network activity

- Surveys/questionnaires as per Ofsted requirements covering

    - students/questionnaires

    - parents/pupils

    - Staff

Governors

Governors are responsible for the approval of the E-Safety policy and for reviewing the effectiveness of the policy. This will be carried out by the relevant governing body receiving regular information about e-safety incidents and monitoring reports. A member of the governing body should take on the role of e-safety governor; this role is could be combined with the safeguarding governor role.

Teaching and learning

Electronic communications are developing rapidly and having many effects on society. Therefore it is important to state what the objectives in ICT and the use of the internet.

Areas of consideration

- Using the internet is part of the curriculum and is a fantastic and necessary tool for learning.
- The internet is part of everyday life for education, business and social interaction. The school has a duty in providing students with quality internet access as part of their learning experience.
- Pupils use the internet widely outside of school and need to learn how to evaluate internet information for themselves and take full responsibility for their safety and experience.
- One of the main reasons schools use the internet is to raise educational standards, to promote achievements through pupils and support professional work of staff.
- Internet access is also a privilege for students who show responsibility and take a mature approach to its use.

Some of the benefits of the internet to education include:

- Access to worldwide educational resources
- Access to information and learning whenever, wherever
- Professional development for staff
- Provides an amazing resource for learning
- Easy contact for staff and students via email
- Prepares students for the business world as the majority of business’ communicate via email.
- Provides vast amounts of multi media opportunities such as videos, pictures and animations
- Access to experts in many fields for pupils and staff.

Managing Information Systems

It is very important that a regular review of security of the whole system from user to internet often takes place. ICT security is a very complex issue and cannot be fully covered within this document. **Local Area Network (LAN) security issues include:**

- Users must act responsibly at all times especially downloading large files this could affect the service others receive.
- All users must take responsibility for their network use.
- Workstations should be secured against user mistakes and deliberate actions
- Servers must be located securely and physical access restricted
- The server operating system must be secured and kept up to date
- Virus protection for the whole network must be installed and current
- Access by wireless devices must be proactively managed, secured and encrypted

The schools broadband network needs to be DFE approved plus monitored by a specialist security command centre.

Areas for consideration

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly
- Personal data sent over the internet or taken offsite will be encrypted
- Portable media may not be used without permission and it’s always a good idea to run an anti-virus/malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school network will be regularly checked.
- The ICT coordinator or network manager will review system capacity regularly
- The use of user logins and passwords to access the school network will be enforced.

Managing filtering

Levels of internet access and supervision should differ depending on the pupils age. Access to the internet must be appropriate for all members of the school community. There be times when pupils require access to specific adult material as part of a supervised project. For instance a course text or set novel might include reference to sex. Staff in school may need to research areas such as drugs, sexual health, bullying, racism etc. In these cases there is a legitimate use and this should be recognised and restrictions moved or temporally removed if blocks are in place. Systems may need to be adapted for teachers and differ depending on the age of the pupil.

Access controls fall into a number of overlapping types commonly described as filtering:

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is major task as new sites appear on a regular basis.
- Dynamic content filtering examines web page content or email for unsuitable words.
- Keyword lists will search filter engines and URL’s for inappropriate results and web addresses.
- Rating systems can be employed and rate each page for sexual, profane, violent or other unacceptable content.
- URL monitoring records the internet sites visited by individual users. Reports can also be produced to investigate incidents.
- Key loggers record all text sent from a workstation and analyse patterns.

It is worth highlighting that thousands of inappropriate websites are created each day and many change URL’s to confuse filtering systems. Staff must be trained adequately to supervise internet access.

It is important that the school community realise that filtering is not 100% effective. There are ways to bypass filters such as proxy websites and using devices such as mobiles or tablets not connected to a network. Mistakes may happen and inappropriate content may be accessed. It is highly recommend students are supervised when using the internet and acceptable use polices are in place. There should be an incident log to report breaches of filtering or when inappropriate content has been accessed. Any material that the school believes is illegal should be reported to the appropriate agencies.

If a school believes a website should be blocked centrally this should be reported to the schools broadband service. Teachers should regularly assess websites or search engines before using them with students. If is important to consider that a site may be appropriate one day then completely change to inappropriate the following day. Close attention should be paid to pop ups as they change regularly and can be inappropriate.

How will email be managed?

For any organisation email is an essential means of communication. Emailing can bring significant educational benefits.

However the implications of email use for the school and pupils need to be thought through and appropriate safety measures put in place. Unregulated email could well provide routes to pupils that bypass the traditional school boundaries.

Once an email is set up a degree of responsibility needs to be delegated to the pupil and this causes a number of issues. Restriction of incoming and outgoing email to approved addresses and filtering for unsuitable content is possible.

The school email system should not be considered as completely private and many schools reserve the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and staff. It is very important that staff understand they should be using a work provided email account to communicate with parents/carers, pupils and other professionals for any school business. It is pivotal staff do not email student/s personal email accounts. This is important for confidentiality, security and to safeguard staff from allegations.

The use of email can give away young persons identity such as joe.bloggs@northamptonshire.gov.uk if possible this generally needs to be avoided for younger pupils, as revealing this information could potentially expose a child to identification by unsuitable people. To set up email accounts safely especially for primary students feel free to contact the E-safety officer for Northamptonshire County Council for further advice. Once again email accounts should not be provided that identify both their first, second, last name and their school. Secondary schools should limit pupils to email accounts approved and managed by the school. For primary schools use of a whole class email or project email may be used. When using external providers to provide students with email systems, schools must pay close attention to the sites terms and conditions as some providers have restrictions of use and age limits for their service.

Areas of consideration

- Pupils may only use approved email accounts for school purposes
- Pupils must immediately tell a designated member of staff if they receive offensive emails.
- Pupils most not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by SLT.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.

- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted
- Schools will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- Staff should not use personal email accounts during school hours or for professional purposes.

Can pupils images or work be published?

The security of staff and pupils is paramount and the publishing of pupil's names and images is not acceptable. Published images can be reused, particularly if large images of individual pupils are shown.

Images of a pupil should not be published without the parents or carers written permission. We will ask permission to publish images of work or appropriate personal photographs at the start of each academic year. Young people need to know the consequences of publishing personal information and images on line. If you are going to use the students name when publishing their photo it should just be their first name only.

Other strategies include using relatively small images of groups of pupils as you are not identifying any individuals. "Over the shoulder" can replace "passport style" photographs but can still show case students work. Special consideration needs to be taken into account when uploading photographs to social media sites via a school account. I would strongly recommend "over the shoulder" shots when showcasing students work. Its important to remember the above when using student photographs on a school or organisations social media account.

Areas of consideration

- Images or videos that include pupils must be selected carefully and should not provide material that could be reused.
- A young persons full name will not be used on websites or a schools social media account.
- Written permission from parents or carers will be obtained before images are used for publicity purposes.
- Pupils work can only be published with their permission or the parents
- Once written consent is obtained it must be kept by the school where, until the image is no longer in use.
- It is worth considering a policy regarding the use of photographic images of children which outlines a number of the areas highlighted above.

Photos or videos being uploaded to social media account

It is extremely important the school community are aware how easily identifiable a young person is wearing a school uniform or from just a picture, the school has a duty of care to minimise such opportunities for people who may wish to contact young people inappropriately. The school should strongly consider requesting parents/carers to refrain from publishing images of young people on the internet such as Facebook especially on events such as sports days, Christmas plays etc. The school community should be promoting the importance of high privacy settings on all social media accounts.

Managing social media

It's important the school community are aware that social media is a fantastic resource if used appropriately but allows the publication of unmediated content. Social networking sites can connect people from all over the world. However users can be invited to view personal information and leave comments often with very limited control. Pupils must be made aware of how dangerous it is to upload personal information. Pupils also need to be reminded on regular basis that once an image or comment is made or posted via social media or an app it becomes extremely difficult to remove that image or comment.

All pupils primary, secondary, staff and parents need to be made fully aware of the risks that go with social networking sites. The whole school community must be made aware of the importance of the material they post online, ensuring and strongly advising that all profiles on social media accounts are set to private. When students set up a social media account up at any age then it is strongly advisable that profile settings are set to high, parents communicate with sons and daughters about the importance of keeping safe using social media, young people only accept friends they know in the real world and they know here to go if they see anything upsetting or someone is persistently asking or making inappropriate comments over the internet.

Areas of consideration

- Pupils will be advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline number, school attended, instant messenger or email address, Blackberry Messenger pin, full names or friends/family, specific interests, clubs etc.

- Pupils will be advised on security and privacy online and will be encouraged often to set privacy settings as high as they can go on any social media site. Also students will be encouraged to set a strong password that only they know, deny access to unknown individuals and block unwanted communications. As highlighted above students will be encouraged to only follow or accept friends they know in the real world.

- All members of the school community will be advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

- Concerns regarding student use of social media including apps will be raised with their parents/carers.

- Students in both primary and secondary schools are advised to save conversations over social media or apps especially if the conversations are distressing them.

- Students are aware of how to report concerns via a social networking site.

- Young people are made aware that images uploaded to a social media account can be very easily copied and pasted.

- The whole school community understand that there is no such thing as delete and almost everything can be traced to the individual or group that up loaded the image or comment.

- **Staff should inform and educate the school community about the risks associated with taking, using, sharing, publicising and distributing images. Students in particular need to recognise the risks of sharing images via mobile phones and social media.**

For advice and support using social media please follow:

http://www.childline.org.uk/explore/onlinesafety/pages/staying-safe-online.aspx

The majority of the advice above also applies for online gaming for further support please follow:

http://www.childline.org.uk/explore/onlinesafety/pages/onlinegaming.aspx

Most social network sites have reporting systems in place to report any content that breaches their terms. If the person responsible has not been identified, or fails to respond to requests to take down the material, the staff member should use the tools on the social networking. See page 22 for support from the UK Safer Internet Centre.

How will the school respond to any incidents of concern?

Internet technologies and electronic communications provide children and young people with exciting opportunities to broaden their learning experiences and develop creativity inside and outside of school. However it is very important to consider the risks associated with the way these technologies can be used. It’s pivotal that an e-safety policy should recognise that children and young people need when using technologies enabling them to keep safe and secure and respect others. It is also important to remember that e-safety risks can be experienced deliberately or unintentially by acting inappropriately or even illegally. Teachers and practitonaners are the first line of the defence and e-safety concerns must be reported via the schools designated safeguarding officer.

It’s also very important that staff share e-safety concerns and observe each other others behaviour. And recognise concerns about pupils and develop a trust so that issues can then be reported.

Where there is cause for concern or fear that illegal activity has taken place or is taking place using computer equipment, schools should report there concerns immediately depending on the level of the concern. Concerns should be reported via the schools or organisations designated safeguarding lead and e-safety lead for the school or organisation. The decision to involve the Police is one that needs to made swiftly.

Recommended incident reporting

In the event of misuse by staff or students, including the use of a school brought electronic device on and off site in an illegal, unsuitable or abusive manor, a report must be made to the head teacher or designated safeguarding officer immediately and the e-safety incident chart below is good model of practice to follow.

In the event of suspicion, all steps in this procedure should be followed

- Have more than one senior member of staff/volunteer involved in the process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Ideally use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure but also the sites and content visited are closely monitored and recorded this will provide further protection.
- Make sure you record the URL of any site containing the alleged misuse and describe the nature of the content causing you concern. If possible record and store screen shots of the machine were the incident has taken place. The information collated should be printed out, signed and dated.
- One this has been completed and fully investigated the safeguarding team and e-safety team or lead will need to judge whether the concern has substance or not. If it does then appropriate action will be required and could include the following:
    - PCSO/Police referral
    - Referral to the MASH team (When there are child protection concerns)
    - CEOP
    - CSE toolkit – To look at the risk of CSE

- If there are any concerns around on line grooming this includes images of child abuse the Police should be contacted immediately.
    - Other circumstances when e-safety concerns should be reported to the Police one discussed with the designated safeguarding officer are highlighted below:
    - Online Grooming
    - Hacking
    - Hate Crime's
    - Harassment
    - Certain types of adult material
    - Other criminal conduct, activity or materials

How will e-safety complaints be handled?

Parents, teachers and pupils should know how to use the schools complaints procedure. The facts of the incident or concern will need to sort and all evidence needs to be compiled where possible and appropriate. E-safety incidents may have an impact on pupils; staff and the wider community both on and off site can have legal and disciplinary consequences.

Other situations could potentially be very serious and a range of sanctions may then be required, which should be then linked to the school disciplinary policy. Safeguarding or illegal issues must be referred to the school safeguarding officer or e-safety coordinator. Advice on dealing with illegal use should be discussed with the Police.

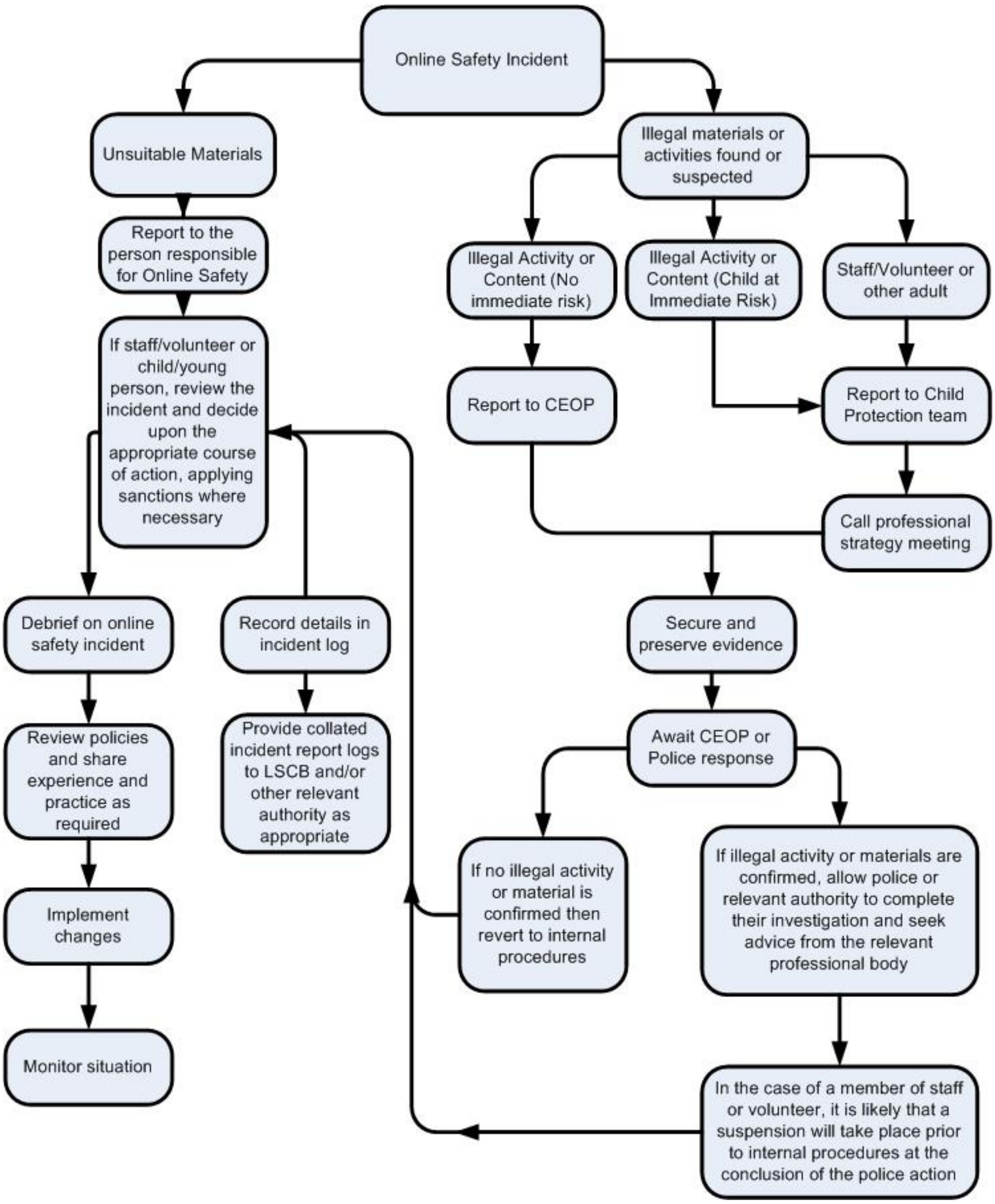
Areas of consideration

- Complaints about internet misuse will be dealt with under the school/organisations complaints procedure.
- Complaints about staff misuse must be referred to the head teacher or director of HR.
- All e-safety incidents and complaints will be recorded by the school, including any action taken.
- Pupils and parents are aware of the complaints procedure.
- It is very important pupils, parents and carers work in partnership with the school or organisation to resolve issues.
- Confidentiality the something the school or organisation community is aware of and the need to follow the schools or organisations procedures for reporting concerns.
- It is recommended that regular discussions are held with the local PCSO, e-safety officer for Northamptonshire County Council and/or the MASH for handling any child protection or illegal issue.

- Any concerns will be dealt with according to the schools disciplinary behaviour and child protection procedures.
- All members of the school or organisation will be reminded regularly about safe and appropriate behaviour on line. And how important it is to not post anything that may cause distress, harm or offence to other members of the school or organisation community.

Incident reporting

In the event of misuse by staff or students, including use of the school network in an illegal, unsuitable or abusive manner, a report must be made to the e-safety coordinator or designated safeguarder immediately and below is an example of an e-safety incident flow chart that can be adopted by the school. **If there is any suspicion that a web site/s may contain child abuse images or any illegal activity a report should be made to the Police immediately.** In the event of minor or accidental misuse, internal investigations should be initiated and disciplinary procedures followed were appropriate.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

The above flow chart is Courtesy of South West Grid For Learning

How will cyberbullying be managed?

It is important to remember that bullying is not a specific criminal offence in the UK where some types of harassing or threatening behaviour or communications could be a criminal offence. There are a number of acts such as the Malicious Communications Act 1988, the Communications Act 2003, Protection from Harassment Act 1997 and the Public Order Act 1986. If a school or organisation feels that an offence has been committed they should seek assistance from the Police.

Cyberbullying is best defined “The use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else”. DCSF 2009

The majority of adults and young people find using the internet and mobile phones a positive and creative part of everyday life. Sadly technologies can also be used in a very negative way. Often when young people are the target of bullying via mobile phones, gaming, social media, apps and chat rooms, they can often feel very isolated and very alone particularly if they feel adults around them don’t understand how cyberbullying is affecting them. A once safe and enjoyable activity and environment can very easily and quickly become threatening, harmful and a major source for anxiety. Therefore it is pivotal that young people, school staff, practitioners, parents and carers understand how destructive cyberbullying can be and how it differs from other forms of bullying. It is very important that promoting a culture of confident users will support online safety.

Often bullying takes place outside the school gates but is usually brought into school and reported. If this is the case it should be reported and acted on. The DFE guidance on Preventing and tackling bullying 2014 states teachers have the power to discipline pupils for misbehaving outside the school premises “to such an extent as is reasonable”. This can relate to any bullying incidents occurring anywhere off the school premises, such as on school or public transport, outside the local shops, or in a town or village centre. Furthermore The Education Act 2011 gives wider search powers to tackle cyber-bullying by providing a specific power to search for and, if necessary, delete inappropriate images (or files) on electronic devices, including mobile phones.

Areas of consideration

- Cyberbullying along with any other forms of bullying by a member of the school community will not be tolerated. Full details should be set out in the schools behaviour or e-safety policy.

- There are clear procedures in place to support a member of the school community that has been affected by cyberbullying including staff.

- As per Ofsted requirements all incidents of cyberbullying are recorded and reported.

- All staff are aware of the clear procedures that are in place to investigate or deal with allegations in relation to cyberbullying.

- The school community are aware that they must keep any evidence of cyberbullying such as print out, screen shots and photos.

- The school will take a number of steps to identify the bully. This could well mean going through the schools monitoring/filtering system to see what has been sent. Victims and perpetrators may have to be interviewed and the Police may have to be involved if necessary.

- Parents, staff and pupils are required to work with the schools to support the schools approach to cyberbullying.

Sanctions for those involved in cyberbullying may include:

- Perpetrator is asked to remove material deemed inappropriate or offensive. Also you can ask the perpetrator to delete the account but ideally have a member of staff as a witness to make sure the account has been closed down.

- Service provider can be contacted and asked to remove the content however if you a reporting something on a social network site you must state how it has broken their terms and conditions.

- Internet access may be suspended for the perpetrator/s for a period of time and other sanctions put in place in accordance with the schools behaviour or e-safety policy.

- Parent and carers will be informed

- The Police may be contacted if there is a suspicion the a criminal offence has been suspected.

School staff being targeted over the internet

School leaders, teachers, school staff, parents and pupils all have rights and responsibilities in relation to cyberbullying and everyone should work together to create an environment in which pupils can learn and develop. Staff have the right to work free from harassment and bullying themselves that has been carried out over the internet. DFE guidance published in 2014 states that schools should also encourage all members of the school community including parents to use social media responsibly. Parents have a right to raise concerns about the education of their child, but they should do in appropriate manor.

It is highly recommended that staff familiarise themselves with the security and privacy settings on social media accounts. It is imperative staff do not give members of the school community easy access to personal information on a social media account. It is also highly recommend that staff employed by the school do not accept parents or students as friends past or present on social media accounts as this could well leave the member of staff/s open to bullying and harassment. Also be aware that a member of staff's social media friends may also be friends with pupils and their family members and could read comments, posts and see pictures if an account does not have appropriate privacy settings. Safe practice for staff using social media needs to be embedded throughout the school.

Staff posting inappropriate comments on social media could lead to disciplinary action and having their employment terminated. Staff need to be aware that their reputation could also be harmed by what others share about them online, such as friends tagging staff in inappropriate posts, photographs or videos. Staff should also not give out personal mobile numbers or email address even for school trips.

If a member of staff has been bullied online or is being bullied online it should be reported immediately to a line manager or senior member of staff. If possible try and keep any evidence and record the date and time. If the perpetrator is known to be a current pupil or colleague the most effective way to deal with it is through the schools disciplinary procedures. If the perpetrator is an adult the fist step is for a senior member of staff to invite them into school for a meeting to discuss their concerns. And if the complaint is reasonable then members of the school community need to be made aware of the correct channels available to air their complaints. A request should be made to remove the information. If the individual refuses to meet or the remove information from the social media account then the following can be explored. You can ask for the content to be removed from the social media site but you must state how its broken there terms and conditions, seek guidance from Northamptonshire County Council E-Safety Officer or seek support from the UK safer internet centre professional hotline 0844 381 4772 or email helpline@saferinternet.org.uk they are open Monday to Friday, 10am to 4pm. If someone is in immediate danger or the comments are abusive, sexual or a hate crime you may want to contact the police ASAP.

Management of mobile phones and tablets

Mobile phones and tablets are now considered to be an everyday item in today's society in both primary and secondary schools. Mobile phones and other internet enabled devices can be used to communicate in a number of ways such as texting, camera phones and internet accesses are all common features.

Mobile phones can cause a number of problems when they are not used appropriately:

- They are valuable items and can be easily stolen or damaged
- They are usually at the heart of cyberbullying
- Internet access through 3G and 4G can allow pupils to bypass the schools wi-fi therefore security settings and filtering systems do not apply.
- They are often put onto silent in a classroom going against classroom discipline
- The vast majority of phones now come with a camera leading to safeguarding concerns and bullying.

Schools often have difficult decision to make when it comes to banning or enabling mobile phones or tablets in schools. Many parents/carers could also be concerned for health and safety reasons if their child were not allowed to carry a mobile phone. Also many staff carry mobiles and tablets within school to keep in touch with staff.

Due to widespread use of personal devices it is essential that schools take appropriate measures to ensure mobile phones and devices are used responsibly in schools. Furthermore it is extremely important that mobile phone and tablet usage does not impede teaching, learning and good order in a classroom. Staff and students must be given clear boundaries and how to use devices professionally.

As highlighted above the use of mobile phones and personal devices is a school decision, however below are some statements you may want to take into consideration when creating an effective policy.

Areas of consideration

- The use of mobile phones and other personal devices by students and staff in school/s will be decided by the school and could be in the school acceptable use of mobile phone policy.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices such as tablets is forbidden by any member of the school community and any breaches will be dealt with as part of the school or organisations disciplinary or behaviour policy.
- Schools and organisations may want to consider confiscating a phone or device such as a tablet if the device had broken or breached the schools behaviour or discipline policy. The phone or device could well end up being searched by a member of SLT with the consent of the pupil or the parent/carer. If there is suspicion that the

material on the mobile or any other electronic device may provide evidence relating to a criminal offence the phone will be handed over to the Police for a further investigation.

- Mobile phones and any other electronic device unless the student/s are using the device as a learning aid will be not be used during lessons or formal school time. They should be switched off at all times.
- In order for a school to make an informed decision on allowing or banning student mobile phone usage during school hours it is recommend that a parental survey is sent out via letter or electronically asking parents to support the decision on mobile phone usage in schools. Once the data is obtained a discussion then needs to take place between the governors and SLT.
- Staff should not use personal mobile phones or electronic devices to take videos of pupils and will only use work provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action will be taken.

Staff Bring Your Own Device (BYOD)

The opportunities offered via mobile technologies are vast as more and more online services become available for teaching and learning. This has led to schools allowing staff to bring in their own device in order to provide a greater choice and usability. However it is important that a number of e-safety considerations for BYOD have been explored. BYOD should not bring in e-safety concerns of issue into what should be a secure environment. Considerations may include secure access, filtering, data protection, storage and the transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. The above is not and exhaustive list.

Areas of consideration

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to data protection acts
- All users are provided with an acceptable use agreement that is signed and dated
- The network is secure and access for users is clearly differentiated
- Where possible the devices will be covered by the schools filtering system whilst being used on the premises.
- Passwords and usernames are kept secure
- Mandatory training is undertaken by all staff
- Students and staff receive regular training on the use of personal devices
- Regular audits are carried out to ensure staff are complaining

- Any device that is lost, stolen, or changed ownership or damaged is reported to the appropriate person.

- Any user leaving the school will be made clear what is expected of them and their device before they leave.

Communication Policy

Many pupils are very familiar with mobile and internet use and it is recommend young people are at the heart of developing positive ways to combat and educate the school community in e-safety especially when designing the school or organisations e-safety policy through the student council or something similar.

As previously highlighted the pupil parent agreement form should include a copy of the school e-safety rules appropriate to the age of the pupil. Once more as per Ofsted requirements e-safety needs to be embedded in the curriculum and can also form part of PSHE lessons.

Useful e-safety programmes and resources include:

- Think u know: www.thinkuknow.co.uk

- Digizen: www.digizen.org

- Kidsmart: www.kidsmart.org.uk

Areas of consideration

- All users must be informed that network and internet use will be monitored

- E-safety will be taught throughout the school to raise the awareness and importance of safe and responsible internet use amongst pupils and staff.

- An e-safety module will be included in the ICT teaching syllabus and PSHE or Citizenship programmes.

- E-safety rules or copies of the student acceptable use policy will be in all rooms with computers.

- Safe and responsible use of the internet and technology will be reinforced across the curriculum and subject areas.

- There must be a focus on e-safety for groups or individuals that are considered vulnerable.

How will parents be supported?

Parents need to be supported as much as possible within e-safety. Unless parents are aware of the dangers, pupils may have access to inappropriate material and/or find themselves in real danger as often there is no filtering in place in the home on the internet or on the device/s being used. With support from the school plans may be able to be put into place to help appropriate and supervised use of the internet at home and educate them on the risks. One effective strategy is to help parents understanding of ICT by running e-safety awareness sessions. Again these can be provided through Northamptonshire County Council's e-safety advisor.

Areas of consideration

- Parents consideration will be drawn to the school e-safety policy through newsletters, prospectus and on the schools website.
- A strong partnership approach to e-safety at home and at school with parents should be encouraged. This may include parent's sessions or holding an e-safety awareness sessions during or alongside another schools event such as parents evening.
- Parents are requested to sign an e-safety/internet agreement as part of the home school agreement.
- Parents will be encouraged to read the school acceptable use policy for pupils and encouraged to discuss it implications with their children.
- Information on e-safety will be made available to parents in a number of formats.
- Advice on useful resources such as websites, filtering within the home, keeping safe using social media, mobile phone technology and gaming will be made available to parents.
- Regular e-safety parent sessions should be held and can be provided through the Northamptonshire County Council e-safety officer.

How should personal data be protected

The quantity and variety of data held is expanding rapidly the use of USB pens has become common place. Whilst storing data can be very useful and convenient, data can be mishandled, stolen or miss misused. Personal data held on a USB must be password protected. If a member of staff needs to take personal data of site a member of SLT must be informed and the appropriate measures highlighted below are put into place.

The Data Protection Act 1998 gives individuals the right to know what information is held about them and provides a framework that personal information is handled properly. Under the Act every organisation should notify the Information Commissioner's Office, unless they are exempt.

The Data Protection Act 1998 applies to everyone that handles or has access to information concerning individuals. Everyone in the work place has a legal duty to protect the privacy of information relating to individuals. The Act set out eight data principle data protection principles, which must be considered when processing personal data. The Act also gives rights to the people the information is about.

The eight principles are that personal data must be:

- Processed fairly lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Held no longer than is necessary
- Processed in line with the individuals rights
- Kept secure
- Transferred to other countries with suitable security measures

Areas of consideration

- Every effort will be made to ensure that data held is accurate and up to date.
- Risk assessments are carried out
- There are clear polices about the use of cloud storage/cloud computing which ensure that such data storage meets the requirements by the Information Commissioners' Office.
- There are clear procedures for and routines for the deletion and disposal of data.
- Staff must ensure they are properly "logged off" when they are working on or using personal data.
- Transferring data must be done so encrypted and secure passwords.
- If using a personal storage device such as a USB stick the device must be password protected.
- When using a laptop, memory stick or any other removable media source to access personal data the laptop has virus and malware checking software.

How are emerging technologies managed?

Many new emerging technologies offer the potential to develop new teaching and learning tools, including mobile communications, internet access, collaboration and multimedia tools. It is highly recommended a risk assessment is undertaken for each piece of technology for effective and safe practice within the school. Until a risk assessment is completed the safest approach is to deny access until safety has been established. It's important to remember virtual online communities widen and enhance learning. The safety and effectiveness depends on users being trusted and identifiable. This becomes difficult when a lot most students access new technologies outside of school time sites such as Facebook, Instagram, YouTube and Twitter. The registering of individuals to establish and maintain validated electronic devices is essential for safe communication but is often not possible. Webcams are very common as is video conferencing enabling videos to be exchanged over the internet. Used appropriately webcams and video conferencing can enhance learning however used inappropriately young people are open to grooming, stalking and hacking to name just a few.

Schools should keep up to date with technologies, including those relating to mobile phones and tablets. For instance young people texting is a frequent activity for many pupils and families; however this could be used to report pupil absence or remind parents about up coming trips.

Pupils may need reminding that inappropriate texts or images conflicts with other school polices.

Areas of consideration

- Emerging technologies will be examined for educational benefits and a risk assessment will be carried out before it's used in school.
- Pupils will be instructed and reminded on a regular basis about the safe and appropriate use of technology and personal devices on and off site in accordance with acceptable use polices.

Acknowledgements

- South West Grid For Learning who have a number of resources around policy writing and acceptable use polices

  http://www.swgfl.org.uk/products-services/Online-Safety-Services/E-Safety-Resources/creating-an-esafety-policy

- Rebecca Avery E-safety officer at Kent County Council

- Department for Education: Cyberbullying advice for head teachers and school staff

Appendix

Useful tool for reviewing a schools e-safety policy

This e-safety policy was approved by the board of Directors/Governing Body/Governors Sub Committee on:	*Insert Date*
The implementation of this e-safety policy will be monitored by the:	*Insert name of group/individual (suggested group/s – E-Safety Coordinator/Officer/Committee, Senior Leadership Team, other relevant group/s)*
Monitoring will take place at regular intervals:	*Insert time period (recommended to be at least once a year)*
The governing board will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include details of e-safety incidents) at regular intervals:	
The E-Safety Policy will be reviewed annually, or more regularly due the ever changing nature of technology, new threats to technology or incidents that have taken place. The review date for policies will be:	*Insert date*
Should serious e-safety incidents take place, the following external persons/agencies should be informed:	*Insert names/titles of relevant persons/agencies e.g Safeguarding Officer, Police, CEOP and MASH. Don’t forget the sexual exploitation toolkit if you feel a young person is at risk of CSE.*