Gedney Church End and Lutton St Nicholas Federated Primary Schools

E-Safety Policy

Contents:

Foreword

The remit for the safeguarding of the child lies with the Local Safeguarding Children's Board (LSCB), and this includes e-safety. LSCB has produced an umbrella e-safety policy, the policy contained within this document is drawn from LSCB and written with federation pupils and staff in mind. This policy and guidance has been produced in conjunction with Lincolnshire County Council and CfBT School Improvement Service with input from a number of other agencies acknowledged below.

Acknowledgements

The following people have been instrumental in developing this policy:

- Rebecca Avery Kent County Council - Esafety Officer
- Dan Hawbrook Lincolnshire County Council - LSCB
- Leigh Middleton Lincolnshire County Council - Legal Team
- Amy Hall Lincolnshire County Council - Legal Team
- Dan Flear Lincolnshire County Council - Risk Team
- Kath Allatt Lincolnshire County Council—National Union of Teachers
- Darren Gelder CfBT School Improvement Service
- John Jefferies CfBT School Improvement Service
- Andrew Dickenson CfBT School Improvement Service
- Rose Roberts CfBT School Improvement Service
- Charlotte Smith CfBT School Improvement Service
- Alan Mackenzie CfBT School Improvement Service, now private provider of e-safety education services
- Di Hoyer NSPCC
- Simon Pickett Welton William Farr C.E. Comprehensive School
- Mark Millinson Boston St Thomas C.E. Primary School
- Nicole Norton Lincolnshire Police - Multi Agency Public Protection
- Caroline Broughton Lincolnshire Police - Youth Policy, Criminal Justice and Partnerships
- Steve Corkin Lincolnshire Police - Community Beat Manager, North Hykeham
- The pupils and staff of the federated schools of Gedney Church End and Lutton St. Nicholas

E-Safety Policy Statement

The use of digital technology is now seen as an essential part of everyday life. The number of SMS (text) messages and emails sent everyday greatly exceeds the population of the planet. Nearly every company, organisation, agency, school and local authority has a presence somewhere on the internet, allowing them to engage different people in different ways. While digital technology can be used in positive ways, it can also be used in extremely negative ways. Paedophiles use this technology to contact, groom and blackmail young people in the virtual world with a view to abusing them in the real world. Children and young people are able to anonymously bully classmates and teachers, while adults may find themselves at greater risk of identity theft should they publish too much information about their life onto a social network.

The risks are real but many people do not see that activity within a virtual world can have an effect in the real world. Comments posted onto social networking sites can lead to education staff being disciplined and young people being bullied. Many are also unaware that some activities in the virtual world are criminal offences and can lead to prosecution.

The Lincolnshire Safeguarding Children Board has overall statutory responsibility for the safeguarding of the child, and that includes the virtual world as well as the real, and takes seriously the role it has to ensure that member agencies co-operate to safeguard and promote the welfare of children and young people in the locality, and to ensure that they are effective in doing so.

Primarily e-Safety is used to describe pro-active methods of educating and safeguarding children and young people while they use digital technology. In order for children and young people to remain safe we will educate them not only in the dangers but also inform them who they can contact should they feel at risk and where to go for advice while still promoting the many benefits of using digital technology, thereby empowering them with the knowledge and confidence of well researched good practice and continuing development.

The large majority of reported incidents involve children being contacted by adults for sexual purposes, visiting highly inappropriate websites or being bullied by their peers through technology. However it should also be remembered that there have been instances where adults have been the victims through a lack of knowledge of the dangers present and by not applying real world common sense to the vast virtual world available to them on the internet.

What is E-Safety?

The federation’s E-Safety Policy reflects the importance it places on the safe use of information systems and electronic communications. Within Lincolnshire, the definition of e-safety is the proactive and reactive measures to ensure the safety of the child, and adults working with the child, whilst using digital technologies. This extends to policy, training and guidance on the issues which surround risky behaviours, and encompasses the technical solutions which provide further safeguarding tools.

It should be remembered that digital technology reaches far and wide, not only computers and laptops, but consideration should also be given to technologies such as: iPads, iPod Touches and iPhones; Xbox 360; Playstations; Nintendo Wii; mobile phones and PDA's, and anything else which allows interactive digital communication online.

E-Safety concerns safeguarding children and young people in the digital world. E-Safety emphasises learning to understand and use new technologies in a positive way.

E-Safety is less about restriction and more about education about the risks as well as the benefits so we can feel confident online. Any approach needs to be rooted in the real world. Our children are being brought up in the digital age therefore restrictions can prejudice their access to the many opportunities it presents. High quality education, however, will help them to be aware of the dangers and exercise common sense and good judgement when using digital technologies online.

E-Safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school. The Internet is an unmanaged, open communications channel. The World Wide Web, email, blogs and social networks all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Some of the material on the Internet is published for an adult audience and can include violent and adult content. Information on weapons, crime and racism may also be unsuitable for children and young people to access. Pupils and staff need to develop critical skills to evaluate online material and learn that publishing personal information could compromise their security and that of others. Our federation has a duty of care to enable pupils to use on-line systems safely. We need to protect ourselves from legal challenge and ensure that staff work within the boundaries of professional behaviour. The law is catching up with Internet developments: for example it is an offence to store images showing child abuse and to use email, text or instant messaging (IM) to 'groom' children.

The federations can protect itself by making it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised" and ensure an Acceptable Use Policy is in place. E-Safety training is an essential element of staff induction and part of an ongoing CPD programme. However, we are aware that a disclaimer is not sufficient to protect a school from a claim of personal injury and the school needs to ensure that all reasonable actions have been taken and measures put in place to protect users.

The rapid development and accessibility of the Internet and new technologies such as personal publishing and social networking means that e-Safety is an ever growing and changing area of interest and concern. The school's e-Safety policy must reflect this by keeping abreast of the vast changes taking place around us.

It is recommended that the federation's e-Safety Policy should be read and applied in conjunction with other policies including Behaviour, Child Protection and Anti-Bullying. E-Safety must be built into the curriculum.

OFSTED

In January 2014, OfSTED published guidance for the inspection of e-safety in schools. This guidance is no longer issued or updated but it remains as useful guidance for schools facing an inspection.

OfSTED view e-safety as the school's ability to:

- Protect and educate pupils and staff in their use of technology
- Have the appropriate mechanisms to intervene and support any incident where appropriate

The associated issues are as follows:

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

Content

- Exposure to inappropriate content, including online pornography, ignoring age-ratings in games, exposure to violence associated with often racist language and substance abuse
- Content validation, how to check authenticity and accuracy of online content

Contact

- Grooming
- Cyber-bullying in all forms
- Identity theft and sharing passwords

Conduct

- Privacy issues including the disclosure of personal information
- Digital footprint and online reputation
- Health and well-being including the amount of time spent online
- Sexting, the sending and receiving of personally intimate images (occasionally referred to as Self-Generated Indecent Images, SGII)
- Copyright, little care or consideration for intellectual property and ownership e.g. music, films, images etc.)

Key Features of Good and Outstanding Practice

Through research and subject-led inspections, OfSTED have been able to collate outcomes to produce recommendations in respect of the common features of good and outstanding practice in schools. This should serve as a guide towards excellence on behalf of the federation and our practice should be regularly checked as a result.

It is the responsibility of the Head Teacher to ensure that this is carried out on a regular basis, supported by the ICT Leader and the wider Governing Body. All aspects of our work will also be subject to external review through the Local Authority Education Advisor, OfSTED and the links that have already been established with private providers and partners.

Whole school consistent approach	▪ All teaching and non-teaching staff can recognise and are aware of e-safety issues ▪ High quality leadership and management make e-safety a priority across all areas of the school ▪ A high priority given to training in e-safety, extending expertise widely and building internal capacity ▪ The contribution of pupils, parents and the wider school community is valued and integrated
Robust and integrated reporting routines	▪ School-based reporting routes that are clearly understood and used by the whole school, for example online anonymous reporting systems ▪ Report abuse buttons, for example CEOP are known by pupils, parents and staff ▪ Clear, signposted and respected routes to key members of staff are known by pupils, parents and staff ▪ Effective use of peer mentoring and support
Staff	▪ All teaching and non-teaching staff receive regular, up-to-date training ▪ One or more members of staff have a higher level of expertise and clearly defined responsibilities
Policies	▪ Rigorous e-safety policies and procedures are in place, written in plain English, contributed to by the whole school, updated regularly and ratified by governors ▪ The e-safety policy should be integrated with other relevant policies such as behaviour, safeguarding and bullying ▪ The e-safety policy should incorporate an Acceptable Usage Policy that is understood and respected by pupils, parents and staff
Education	▪ An age-appropriate e-safety curriculum that is flexible, relevant and engages pupils' interest; that is used to promote e-safety through teaching pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety ▪ Rewards are used to cultivate positive and responsible use ▪ Peer mentoring programmes are established
Infrastructure	▪ A recognised Internet Service Provider (ISP) or Regional Broadband Consortium (RBC) together with age-related filtering that is actively monitored
Monitoring and Evaluation	▪ Risk Assessment is taken seriously and used to good effect in promoting e-safety ▪ Using data effectively to assess the impact of e-safety practice and how this informs strategy
Management of Personal Data	▪ The impact level of personal data is understood and data is managed securely and in accordance with the statutory requirements of the Data Protection Act (1998) ▪ Professional communications between the school that utilise technology should take place within clear and explicit professional boundaries, be transparent and open to scrutiny and personal information should never be shared with a child

	or young person

OfSTED Led Research and Recommendations (March 2015)

During March 2015, OfSTED conducted an HMI-led survey that referenced a discussion with senior leaders, staff and governors across 39 primary schools and 45 secondary school inspections. This served as a follow-on from the 2010 report 'The Safe Use of New Technologies', led by David Brown (HMI).

The key outcomes are as follows:

- Over 25% of secondary students cannot recall if they have been taught about online safety in the last 12 months
- 5% of schools do not have an Online safety Policy in place
- Only 74% of students were aware that they had an Online Safety Policy
- A significant majority of schools still do not allow the use of personal devices
- A significant majority of schools do not involve a student contribution, despite this being a key indicator of outstanding practice
- Assemblies and computing/ICT lessons are the main focus for online safety teaching for many schools although PSHE lessons play a significant role in the delivery of key findings and messages
- There is still inconsistency in the provision of an Online Safety Curriculum of breadth with progression
- Just over 25% of secondary students lack confidence in their teacher's knowledge of online safety issues
- Staff training remains inconsistent and what senior leaders might see as training is not reflected by the staff. Staff feedback suggests that training is often reactive, being delivered after an incident has taken place.
- Staff have confidence in recognising, responding to and resolving online safety issues. This is slightly stronger in secondary schools than primary schools.
- Reporting is the weakest area of school practice

In our policy and practice, we seek to ensure that all such recommendation are taken into account and fully implemented for the benefit of all pupils.

The Responsibilities of Federation Staff

Information technologies are developing rapidly and can leave staff unsure of best practice or how to discuss e-Safety issues with pupils. Further advice can be sought from Lincolnshire Safeguarding, from CfBT ICT consultants or our designated provider of ICT technical support services (Ark ICT Solutions).

The trust between pupils and federation staff is essential to education but very occasionally it can break down. This is not new, but has been highlighted by better awareness of human failings and greater respect for children. Nationally, the Child Exploitation and Online Protection Centre (CEOP) was set up by the Home Office to safeguard children's online experiences and relentlessly track down and prosecute offenders and their work should be acknowledged and built upon by the federation.

Within our federation, a member of staff who flouts security advice or uses ICT technology for inappropriate reasons risks dismissal through the staff disciplinary processes. All staff should sign an Acceptable Use Policy on appointment. Staff thereby accept that the school can monitor network and internet usage to help ensure staff and pupil safety.

Staff that manage filtering systems or monitor ICT use have great responsibility and must be appropriately supervised. Procedures define how inappropriate or illegal ICT use is reported to the Senior Management Team. Staff must be aware of dangers to themselves in managing ICT use, for instance in viewing inappropriate images to investigate their source.

Email, text messaging, Social Networking and Instant Messaging (IM) all provide additional channels of communication between staff and pupils. Inappropriate behaviour can occur and communications can be misinterpreted. Staff should be aware of the power of the Police to identify the sender of inappropriate messages. Schools should provide establishment email accounts for all staff.

Staff should be aware that students may be subject to cyber-bullying via electronic methods of communication both in and out of school. The Head Teacher understands that he has the power “to such an extent as is reasonable” to regulate the conduct of pupils off site (Education and Inspections Act 2006).

If there is any suspicion of illegal activity staff should NEVER investigate themselves but must report to Lincolnshire Police as soon as possible via the Head Teacher.

E-Safety Policy: Federation Staff

Internet access

You must not access or attempt to access any sites that contain any of the following:

- child abuse;
- pornography;
- promoting discrimination of any kind;
- promoting racial or religious hatred;
- promoting illegal acts;
- any other information which may be illegal or offensive to colleagues.

It is recognised that under certain circumstances inadvertent access may happen. For example, a class researching the holocaust may produce results with Nazi propaganda. Should you or a pupil access any of these sites unintentionally you should report the matter to a member of the Senior Management Team so that it can be logged.

Access to any of the following should be reported to Lincolnshire Police:

- Images of child abuse (sometimes incorrectly referred to as child pornography).

These are images of children apparently under 16 years old involved in sexual activity or posed to be sexually provocative; adult material that potentially breaches the Obscene Publications Act

- Criminally racist material in the UK.

Social networking

All social networking has been blocked at both schools.

The following paragraphs have been taken from the staff handbook, which is updated and circulated to all federation staff on an annual basis:

Facebook, Twitter and other forms of social media can be the cause of much distress and anxiety within a school context and point to the importance of safe Internet protocols being established within the federation. While it is inappropriate to forbid staff from using such media, the following guidance is issued with the expectation that it is followed in full:

- All matters that occur within school are confidential and must not become subject to discussion online
- No image taken at school can be published online unless permission has been sought from Mr. Whitney beforehand; if in doubt, please ask
- No communication with children via the internet is permitted including adding them as friends and/or followers; any such requests must be referred back to Mr. Whitney immediately
- Adding parents as friends and/or followers is also discouraged as we are seeking to develop professional and not personal relationships
- Privacy settings should be maximised as basic information can still be collected about members of staff without the necessity of forming friendships therefore profile pages will need to be carefully considered; any inappropriate content could compromise the member of staff concerned
- Any activity online is recorded within the server networks of each ISP therefore staff need to carefully consider the nature of their Internet use and how this can compromise their position as professionals within the wider community

Mr. Whitney is very happy to provide advice in this difficult and sensitive area and all staff are reminded of the Local Authority’s safe Internet guidance and the sanctions that can result from inappropriate use either at school or home. An e-safety audit has been completed and this will lead to the development of specific federation policy in this important area.’

Use of E-mail

All members of staff should use their professional email address for conducting federation business. Use of federation e-mail for personal/social use is at the discretion of the Head Teacher.

Passwords

Staff should keep passwords private. Passwords are confidential and individualised to each person. On no account should a member of staff allow a student to use a staff login.

Data Protection

Where a member of staff has to take home sensitive or confidential information sufficient safeguards should be in place to prevent loss or misuse, i.e. is it really necessary to take it all home, can it be encrypted, does it have to be on a USB memory stick which can be easily misplaced.

File sharing

Technology such as peer to peer (P2P) and bit torrents is not permitted on the Lincolnshire School's Network.

Personal Use

Staff are not permitted to use ICT equipment for personal use unless federation policy allows otherwise. If personal use is permitted, the federation should emphasise what is considered within the boundaries of acceptance.

Images and Videos

Staff and pupils should not upload onto any internet site images or videos of themselves, other staff or pupils without consent.

Use of Personal ICT

Use of personal ICT equipment is at the discretion of the Senior Management Team. Any such use should be stringently checked for up to date anti-virus and malware checkers.

Viruses and other malware

Any virus outbreaks are to be reported to Ark ICT Solutions (0845 459 4900) as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the federation.

E-Safety Policy: Pupils

The use of ICT within schools has enormous benefit but there are reasons why the federation and Local Authority must put some restrictions in place, such as:

- ICT equipment is very expensive to buy and maintain;
- the federation and Local Authority have a duty of care to ensure that you are safe and that you are not exposed to illegal or inappropriate content.

Use of the Internet

The internet is provided to help you with learning activities such as research, online activities, online educational games and many other things. The internet is not to be used to access anything which is illegal, or anything that someone else may find offensive.

This would include:

- pornography;
- discrimination;
- any images or documents that promote racial or religious hatred.

If you are unsure, or if you come across anything you feel is inappropriate, you should turn your computer monitor off and let your teacher know. Never try to bypass the security by using proxy sites, these are all monitored.

Logins and Passwords

Every person has a different computer login and password. You should never allow anyone else to use your details. If you think someone else may have your details you should have your password changed.

User Areas

Your user area is provided for you to save school work. It is not to be used to save music or other files that you have brought in from home.

Social Networking

Social networking sites are blocked in both schools. Staff will work alongside your parents to ensure your online safety and the following advice will help:

- You should never upload pictures or videos of others without their permission. It is not advisable to upload pictures or videos of yourself, videos and pictures can easily be manipulated and used against you. You should never make negative remarks about the school or anyone within the school. Always keep your personal information private to invited friends only and never post personal information such as your full name, date of birth, address, school, phone number etc. Consider using a nickname and only inviting people you know.
- Universities and future employers have been known to search social networking sites prior to making a place or employment offer

- Beware of fake profiles and people pretending to be somebody else. If something doesn't feel right follow your instincts and report it to an appropriate adult. Never create a false profile as a joke and pretend to be somebody else. This can have serious consequences.
- Some social networking sites have a chat facility. You should never chat to anyone that you don't know or don't recognise.
- It is strongly recommended that you never meet a stranger after meeting them online. If you do, always inform your parents and take one of them with you.

Staff are aware that age restrictions apply to the majority of social networking sites and will bring this information to the attention of your parents.

Security

You should never try to bypass any of the security that is in place. This includes using proxy bypass sites. This security is in place to protect you from illegal sites, and to stop others from hacking into other people's accounts.

Copyright

You should never take information from the internet and use it as your own. A lot of information is copyrighted, which means that it is owned by somebody else and it is illegal to use this information without permission from the owner. If you are unsure, ask your teacher.

Etiquette

Every pupil within the federation has an e-mail address. Remember to always be polite and don't use any bad language. Consider what you are saying, and how it might be read by somebody else. Without emoticons it is difficult to show emotions in things like emails and blogs, and some things you write may be read incorrectly.

Mobile Phones

Some modern mobile phones offer the same services as a computer, i.e. Facebook, YouTube, email access etc. This can be a great way of keeping in touch with your friends and family but, in the same way that some internet services can be used inappropriately, the same is true with mobile phones.

Never take inappropriate pictures of yourself and send to your friends or upload onto social networking sites. Never forward inappropriate pictures that you have received from somebody else. In some circumstances this can be an illegal act.

Useful websites

- CEOP is a part of the UK police force dedicated to the eradication of child sexual abuse. There is an excellent educational programme, as well as advice and videos for all ages on their website: www.ceop.gov.uk

- IWF (Internet Watch Foundation) provides the UK hotline to report criminal online content: www.iwf.org.uk

- BBC - a fantastic resource of e-safety information for the younger child: www.bbc.co.uk/cbbc/help/web/staysafe

- Cybermentors is all about young people helping and supporting people online: www.cybermentors.org.uk

- Digital citizenship is about building safe spaces and communities, understanding how to manage personal information, and about being internet savvy - using your online presence to grow and shape your world in a safe, creative way, and inspiring others to do the same: www.digizen.org

What To Do and What Not To Do

- Never give out personal details to online friends that you don't know offline.
- Understand what information is personal: i.e. email address, mobile number, school name, sports club, meeting up arrangements, pictures or videos of yourself, friends or family.
- Small pieces of information can easily be pieced together to form a comprehensive insight into your personal life and daily activities.
- Think carefully about the information and pictures you post on your profiles. Once published online, anyone can change or share these images.
- It can be easy to forget that the internet is not a private space, and as result sometimes people engage in risky behaviour online.
- Don't post any pictures, videos or information on your profiles, or in chat rooms, that you would not want a parent or carer to see.
- If you receive spam or junk email and texts, never believe the content, reply to them or use them.
- Don't open files that are from people you don't know. You won't know what they contain—it could be a virus, or worse - an inappropriate image or film.
- Understand that some people lie online and that therefore it's better to keep online mates online.
- Never meet up with any strangers without an adult that you trust.

Don't forget, it is never too late to tell someone if something or someone makes you feel uncomfortable.

Training

It is recognised that digital technologies, pupils' awareness and the level of online risk is constantly evolving and changing. It is the responsibility of senior staff to ensure that regular training is in place for all staff so that they can carry out their duties with safety as the primary consideration. Training will also be used to equip staff with the necessary knowledge, skills and understanding to appropriately support all pupils in their use of digital and online technologies. It is fully recognised that a reactive component will be required as this enables pupils to be supported on an incident-by-incident basis, but the best form of training is preventative, ensuring that pupils have the necessary toolkit of skills to stay safe online and to make positive choices when they encounter challenging situations. As with all training, it is expected that staff evaluate this through the provision of feedback and this will help the Senior Management Team to ensure that all training needs are met on an ongoing basis.

Teaching

The Computing curriculum is planned on a medium-term basis and it is the responsibility of all staff to ensure that the National Curriculum is covered in full at Key Stages 1 and 2. As part of the planning process, staff will consider which aspects of e-safety are relevant to the unit that is being delivered. An e-safety lesson will be delivered at the beginning of each unit and as a result, staff will receive regular e-safety support through the taught curriculum. Assemblies and PSHE lessons will also be used to highlight key issues and the steps pupils can take to stay safe online. Finally, at least once a year, external providers will be used to hold e-safety workshops in school for pupils and also evening sessions for parents. In this way, the importance of e-safety is highlighted and both pupils and parents will be equipped with contemporary information that can help to promote safe Internet use at all times.

Monitoring and Evaluation

The federation's E-safety Policy is subject to monitoring and evaluation and the following strategies will be used to ensure its effectiveness:

- The policy will be reviewed regularly by the Governing Body
- A nominated governor with responsibility for the Computing and e-safety will be appointed and they will be expected to visit the school at least 3 times per year to observe the work of the federation in the classroom. At least 2 meetings will be scheduled with the Computing Subject Leader and 1 meeting with the Head Teacher will also be expected, cross-referenced with current safeguarding requirements.
- The Head Teacher will ensure that the training requirements for all staff are met on an ongoing basis and that a strategic overview of provision is supported by the training that has been provided. To this end, feedback from staff will be collated by the Head Teacher and used to fully support this analysis. Finally, it will be the Head Teacher's responsibility to ensure that the E-safety Policy is regularly updated, in-line with national and federation requirements.
- The Computing Subject Leader will monitor and evaluate the implementation of the E-safety Policy and make recommendations to the Head Teacher as and when required
- Teaching staff will regularly contribute to policy review on the basis of their experience in the classroom and the responses of pupils and parents
- Pupils, School Councillors and Peer Mentors will also be involved in the monitoring and development of provision through the feedback they provide, a record of the support they have received/offered and also their wider experiences within the classroom and beyond

- Parents will contribute to the monitoring of policy and practice through regular, targeted surveys, ongoing feedback, attendance at workshops, support for home learning and a further strengthening of the links between home and school

Signed by Head Teacher:

Ratified by Governors: May 2012

Last Updated: November 2015

Appendix A

Thoughts and Recommended Next Steps

Technology

The two technology tools available to schools to provide assistance in safeguarding are internet filtering and Securus behaviour management.

Internet filtering - take some time to discuss with your technical team or your managed service provider which categories are blocked and which are allowed. Who makes the decision to block or unblock? Is it the technical team or those delivering the curriculum? Are your staff and students being overly blocked through a "locked down" system or is the system being properly managed? Are there steps in place to have internet sites blocked or unblocked quickly? What do the students think? Do they feel they are being overly blocked? Does your school run regular reports to see if there has been any inappropriate activity?

Securus Behaviour Management - this is a new tool which has recently become available to all schools for free (with a one-off training cost). It can help protect students from cyber bullying, grooming, racist and harmful behaviour. The software takes a screenshot of anything it believes may be inappropriate or illegal, based upon pre-defined rules and threshold levels. It then emails this screenshot to a selected person within the school. If your school has this installed, are both staff and students monitored? If you don't have it installed you should give it serious consideration.

Policies

It is recommended that the federation's e-Safety Policy should be read and applied in conjunction with other policies including Behaviour, Child Protection and Anti-Bullying. E-Safety must be built into the curriculum.

Training

Are all staff aware of e-safety, not just teaching staff? Are the students aware? You must be aware of your duty of care as a school, and also your requirements under OFSTED. Are there e-safety training and awareness sessions available for staff, students and parents? If your school is not confident, consider contacting CfBT and using its accredited training sessions.

Guidance

Technology moves at such a pace, and risk taking behaviours evolve into other risks. Ongoing training and guidance, particularly as part of CPD is a must. Have you signed up to the monthly e-Safety newsletter which will keep you up to date with other training initiatives?

Responsibility

This lies with the Head Teacher and governing body. Are you aware of your responsibilities and duty of care? Has this responsibility been devolved to the technical team? If so, why? These are not technical issues but potentially very serious pastoral ones.

Appendix B

Inappropriate Activity Flowchart

(Copy provided)

Appendix C

Illegal Activity Flowchart

(Copy provided)