Primary eSafety Framework Document

Gillibrand Primary School

2012

Developing and Reviewing this Policy

This eSafety Policy has been written as part of a consultation process involving the following people:

Ms Sharon Bryson (Head Teacher)

Mrs Ashley Clayton (Deputy Head Teacher)

Miss Abigail Keane (ICT Subject Leader)

Miss Linda Craven (SLT)

It has been approved by Governors and will be monitored and reviewed as listed below:

Policy Created - Date: May 2012

The implementation of this policy will be monitored by: Abigail Keane and Sharon Bryson

This policy will be reviewed as appropriate by **Ms Sharon Bryson** (Head Teacher)

Mrs Ashley Clayton (Deputy Head Teacher)

Miss Abigail Keane (ICT Subject Leader)

Miss Linda Craven (SLT)

Approved by …… (Head Teacher) Date ……

Approved by …… (Governor) Date ……

Contents

eSafety Policy 2012 - Gillibrand Primary School

1. Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective eSafety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our eSafety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings. The policy is organised in 4 main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection.

2. Vision for eSafety at Gillibrand Primary School.

At Gillibrand Primary School, we use technology when appropriate to enhance the learning experience for our children and to support the daily organisation and administration tasks carried out by school staff.

Keeping members of our school community safe, whilst using technology is a priority and we expect staff to act as role models in their use of technology and abide by the shared decisions reflected in our eSafety policy. Children are encouraged to explore and make responsible decisions regarding their uses of technology, informed by 'education' as opposed to the imposition of restrictions. As children are engaging with 21st Century technologies both inside and outside of school, we will provide opportunities for both children and the wider community to understand and view eSafety education as a key life skill.

Our eSafety Policy defines what we consider to be acceptable and unacceptable behaviour regarding the uses of technology in school and the sanctions or procedures to be followed should breaches of security

occur. It is communicated to staff, governors, pupils and parents and is updated in light of the introduction of new technologies or incidents.

3. The role of the school's eSafety Champion.

Our eSafety Champion is Ms Sharon Bryson.

The role of the eSafety Champion in our school includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school's eSafety Policy and associated documents. Including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an eSafety incident occur.
- Ensuring the eSafety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with eSafety issues and guidance through liaison with the Local Authority Schools' ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging eSafety advice/training for staff, parents/carers and governors.
- Ensuring the SLT, staff, pupils and governors are updated as necessary.
- Liaising closely with the school's Designated Senior Person/ Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.

4. Policies and practices

This section of the eSafety Policy sets out the school's approach to eSafety along with the various procedures to be followed in the event of an incident.

This eSafety policy should be read in conjunction with the following other related policies and documents:

4.1 Security and data management

In our school, data is kept secure and all staff are informed as to what they can/cannot do with regard to data in the following ways:

- Key information / data is mapped and securely stored on the main office computer. This is accessible only by the bursar and head teacher.
- The head teacher has overall responsibility for managing all information.
- Staff have been informed of the location of all data relevant to them by the head teacher.
- Staff have been informed of their legal responsibilities with respect to principles of the Data Protection Act (1988) and ensure all data is :
    1. Accurate
    2. Secure
    3. Fairly and lawfully processed
    4. Processed for limited purposes
    5. Processed in accordance with the data subject's rights
    6. Adequate, relevant and not excessive
    7. Kept no longer than necessary
    8. Only transferred to others with adequate protection

Our school ensures that data is appropriately managed both within and outside the school in the following ways:

- School's equipment, including teacher laptops, must only be used for school purposes and do not contain personal information e.g. personal images, personal financial details, music downloads, personal software. Computers are accessed via a safe username and password and it is the responsibility of the individual to keep this secure at all times. Any breaches in security must be reported immediately to Sharon Bryson.
- School equipment must not be used, for example for online gambling, dating websites, home shopping, booking holidays, and social networking BOTH at home and in school.
- Staff are aware of the school's procedures (eSafety) for disposing of sensitive data, e.g. shredding hard copies, deleting digital information, deleting usernames and passwords from school's VLE, deleting email accounts, IEP, PIPs, SATs information and know the person responsible should there be any queries.
- The school's policy for removal of sensitive data prior to disposal or repair of equipment is documented in eSafety and all staff are aware of the person responsible.
- Remote access is available to SLT and they are only allowed to access data from home via a secured wireless connection. School data must NOT be stored on personal equipment, e.g. home computer or mobile phone.

4.2 Use of mobile devices

All staff are aware that some mobile devices e.g. mobile phones, games consoles or net books can access unfiltered internet content. Staff who bring their mobile phones to school are aware of the correct procedures when using it and children who also choose to bring games consoles into school on appropriate days do so at their own risk.

All devices e.g. USB sticks are both checked at home and on the school system. The system runs a check when a device is connected and will highlight any problems with the mobile device.

Members of staff are aware that the use of mobile phones within school are to be used outside lesson times.

4.3 Use of digital media

In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.

Various forms of digital media offer substantial benefits to education but equally present schools with challenges particularly regarding posting or sharing media on the Internet, through mobile technologies and Social Network sites.

To ensure all users are informed and educated about the risks surrounding taking, using, sharing, publishing and distributing digital media. Our school considers the purpose for which the image will be used e.g. website, brochure or display.

As photographs and videos of pupils and staff are regarded as personal data in terms of The Data Protection Act (1998) we must have written permission for their use from the individual and/or their parents or carers.

Our school seeks consent from the pupil, parent/carer or member of staff who appears in the media or whose name is used. We obtain the parental/carer permission on entry to the school, it is the parents/carers responsibility to highlight any changes to the school bursar.

We do not retain any images of pupils after they have left the establishment.

Staff and pupils are aware that full names and personal details will not be used on any digital media, particularly in association with photographs.

Parents/carers who have been invited to attend school events are allowed to take videos and photographs. They are made aware of any conditions in advance that it is for their own personal use and should not be put online.

In accordance with the Data Protection Act 1998, the school seeks parental consent to take photographs and use video recorders. Photographs are stored on the server and the administration system. Both are password protected.

The schools digital camera/s or memory cards must not leave the school setting unless on an official school trip. Photos are printed/uploaded in the setting by staff and once done images are then immediately removed from the cameras memory at the end of each term.

All staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites.

School ensures that photographs/videos are only taken using school equipment and only for school purpose. School ensures that any photographs/videos are only accessible to appropriate staff/pupils.

School does not allow staff to store digital content on personal equipment. When taking photograph staff ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted. Staff, parents/carers and children are made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved.

The guidelines for safe practice relating to the use of digital media, as outlined in the school's policy are monitored regularly by the ICT coordinator particularly when new members of staff or pupils enter the school. New members of staff are made aware of the eSafety policy and new pupils to the school are given guidelines to positive use of ICT and an image consent form which reflects our school's context and policy.

4.4 Communication technologies

Email:

In our school the following statements reflect our practice in the use of email:

- It is recommended that all users have access to the Lancashire Grid for Learning service as the preferred school e-mail system.
- Only official email addresses should be used to contact staff/pupils.
- The Lancashire Grid for Learning filtering service should reduce the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of SPAM should be reported to the Westfield Centre.
- All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts e.g. Hotmail or Gmail, in school.

- All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

Social Networks:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites:

- Staff must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
- Staff must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- If a Social Network site is used, details must not be shared with pupils and privacy settings be set at maximum.
- Pupils must not be added as 'friends' on any Social Network site.

Remember; whatever means of communication you use you should always conduct yourself in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever.

Mobile telephone:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Mobile telephones:

- School allows personal mobile phones to be used in school by staff outside lesson time and staff bring mobile phones into the establishment at their own risk.
- It is acceptable to use personal mobile phones for school activities e.g. school trips as a mean of communication to and from school/members of staff.
- It is not acceptable to use personal mobile phones to support lessons.
- It is not acceptable to use personal electronic devices to take pictures of children.

Instant Messaging:

Instant messaging, e.g. MSN, Skype, Yahoo Messenger, is a popular communication tool with both adults and children. It provides an opportunity to communicate in 'real time' using text, sound and video. The Lancashire Grid for Learning filtering service 'blocks' these sites by default, but access permissions can be changed at the request of the Headteacher.

In our school the following statements outline what we consider to be acceptable and unacceptable use of Instant Messaging:

- Staff and children are aware of the risks involved using technology e.g. viewing inappropriate images or making unsuitable contacts therefore supervision is paramount.
- They wish to use the secure messaging, forum or chat systems within their VLE (e.g. Moodle)

Virtual Learning Environment (VLE) / Learning Platform:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Virtual Learning Environments:

- Each class teacher has access to the Moodle site to monitor the content that is be added to the learning platform.
- Every teacher has access to Moodle but the ICT coordinator has administration privileges.
- Usernames and passwords are issued to the children, and security is maintained by promoting positive privacy of password protection.
- Pupils are limited to their year group/teacher area where the correct level of work is set according to their topic in class.
- Pupils are taught to use the communication tools in a responsible way in conjunction with the eSafety curriculum.
- Accounts are deleted when staff and pupils leave the school. This is monitored regularly by the ICT coordinator.

Web sites and other online publications

In our school the following statements outline what we consider to be acceptable and unacceptable use of Websites and other online publications:

- Our school website is effective in communicating eSafety messages to parents and carers. There are a lot of resources on there for parents/carers to view and go to for guidance.
- Everybody in the school is aware of the guidance for the use of digital media on the website.
- Everybody in the school is aware of the guidance regarding personal information to the website.
- The ICT coordinator and Head teacher have access to edit the school website and the information is current also they have the overall responsibility for what appears on the website.
- Content on the school website is subject to copyright/personal intellectual copyright restrictions
- The information on the school website is available for everybody to see.
- Downloadable materials are in a read-only format (PDF) where necessary, to prevent content being manipulated and potentially re distributed without the school's consent.

Video conferencing:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Video conferencing:

- A permission letter will be made available for parents/carers to sign giving permission for their child/children to participate in video and photographs (Children will not be appearing 'live' on the Internet through video conferencing link. However, it is still important to remember that the images which are broadcast from school could be captured as a snapshot or video clip from a system receiving the broadcast.)
- The Head Teacher must be obtained in advance of the video conference taking place. All sessions should be logged including the date, time and the name of the external organisation/person(s) taking part.
- Pupils using video conferencing equipment should be supervised at all times.
- All staff supervising video conferencing equipment should know the procedures to follow if they are unhappy with the content of a VC session e.g. how to 'stop' or 'hang up' the call.
- Copyright , privacy and Intellectual Property Rights (IPR) legislation will be breached if images, video or sound are recorded without permission.

Others:

The school will adapt/update the eSafety policy in light of emerging new technologies and any issues or risks associated with these technologies e.g. Bluetooth and Infrared communication.

4.5 Acceptable Use Policy (AUP)

An Acceptable Use Policy is intended to ensure that all users of technology within school will be responsible and stay safe. It should ensure that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.

AUPs are recommended for Staff, Pupils and Visitors/Guests and must be signed and adhered to by users before access to technology is allowed. The agreement is a partnership between parents/carers, pupils and the school to ensure that users kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology must be kept in school and made available to the staff.

AUPs must:

- Be understood by the individual user and relevant to their setting and purpose.
- Be regularly reviewed and updated.
- Be regularly communicated to all users, particularly when changes are made to the eSafety Policy/AUP.
- Outline acceptable and unacceptable behaviour when using technologies, for example:
    - Cyberbullying
    - Inappropriate use of email, communication technologies and Social Network sites and any outline content.
    - Acceptable behaviour when using school equipment/accessing the school network.
- Outline the ways in which users are protected when using technologies e.g. passwords, virus protection and filtering.
- Provide advice for users on how to report any failings in technical safeguards.
- Clearly define how monitoring of network activity and online communications will take place and how this will be enforced.
- Outline sanctions for unacceptable use an make all users aware of the sanctions LINK WILL BEHAVIOUR POLICY.

- Stress the importance of eSafety education and its practical implementation.
- Highlight the importance of parents/carers reading and discussing the content of the AUP with their child.

4.6 Dealing with incidents

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Head Teacher who must refer this to external authorities, e.g. Police, CEOP, and Internet Watch Foundation (IWF). **Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence.** It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Always report potential illegal content to the Internet Watch Foundation. They are licensed to investigate – schools are not!

Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

5. Infrastructure and technology

Pupil Access:

Filtering services within school offer high level of protection but occasionally unsuitable content may get past the filter service. Sophos Anti-Virus software is included in the school's subscription.

Pupils have regular access to computers and are trusted to use them safely and securely. When pupils are accessing the schools equipment and online materials they work alongside a trusted adult.

Passwords:

All staff are aware of the guidelines and importance of password security. Users on the school network have a secure username and password that can be changed regularly. All new and old staff are added and deleted from the system when they start or leave school.

The administrator password for the school network is available to the ICT Subject Leader and other nominated senior staff. All pupils and staff are reminded about the importance of keeping passwords secure and updating them regularly is paramount.

Software/hardware:

In school we have all legal ownership of the software and this is reflected on the licenses that we hold. We have an up to date record of appropriate licenses for all software and who is responsible for maintaining this. There are audits completed of software that we have in school. From this audit we are able to see if there is any software that needs updating or replacing. Between the ICT Subject Leader and the ICT Technician they install appropriate software onto the school system. The teaching staff at school also may suggest programs they have used and they are then installed onto the system if whole school agree.

Managing the network and technical support:

All servers and cabling is securely located and physical access is restricted. The Head Teacher, ICT Subject Leader and ICT Technician are responsible for managing the security of the schools network and server. The computer system is regularly up dated with critical software updates run every Friday. All users have clear defined access right to the school network. There are usernames and passwords set and permissions are assigned depending on the user. Staff and pupils are required to log out of a school system when the computer is left unattended. Users are not allowed to download executable files or install software unless it is to run a program that is used often in school. Users are to report any suspicion or evidence of a breach of security. They are to pass it on to the ICT Subject Leader who will then work with the Head Teacher to deal with the situation. In extreme cases users are to report any breach of security straight to the Head Teacher. All network monitoring that takes place is in accordance with the Data Protection Act 1998. All staff are made aware of all network monitoring and/or remote access that takes places and by whom. All internal/external technical support providers are aware of our schools requirements and standards regarding eSafety. The Head Teacher and Subject Leader are responsible for liaising with and managing the technical support staff.

Filtering and virus protection:

School is aware that they can request devolved control over the LGfL filtering system service if needed. Filtering is managed by county allowing sites that have been checked through onto the school system. Information regarding devolved filtering is stored in the office. It is available for any new member of the SLT. Devolved filtering is communicated to staff at staff meetings where minutes are taken. Staff are aware of the procedures

for blocking and unblocking specific websites and of the procedures for reporting suspected or actual computer virus infections.

6. Education and Training

In 21st Century society, staff and pupils need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that pupils are taught to be responsible and safe users of technology, being able to recognise potential risks and knowing how to respond.

Education and training are essential components of effective eSafety provision. Equipping individuals, particularly pupils, with the appropriate skills and abilities to recognise the risks and how to deal with them is fundamental. eSafety guidance must be embedded within the curriculum and advantage taken of new opportunities to promote eSafety.

Area of risk	**Examples of risk**
Commerce: Pupils need to be taught to identify potential risks when using commercial sites.	Advertising e.g. SPAM Privacy of information (data protection, identity fraud, scams, phishing) Invasive software e.g. Virus", Trojans, Spyware Premium Rate services Online gambling
Content: Pupils need to be taught that not all content is appropriate or from a reliable source.	Illegal materials Inaccurate/bias materials Inappropriate materials Copyright and plagiarism User-generated content e.g. YouTube, Flickr, Cyber-tattoo, Sexting
Contact: Pupils need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	Grooming Cyberbullying Contact Inappropriate emails/instant messaging/blogging Encouraging inappropriate contact

6.1eSafety across the curriculum

It is vital that pupils are taught how to take responsible approach to their own eSafety. Our school provide suitable eSafety education to all pupils. We provide regular, planned eSafety teaching within the range of curriculum areas. We have additional focus on eSafety during the National eSafety Awareness Week. eSafety education is differentiated for pupils with additional educational needs. We ensure pupils are made aware of the relevant legislation when using the Internet e.g. Data Protection Act (1998) and copyright implications by teaching them this through eSafety lessons. Pupils are made aware of the impact of Cyberbullying and how to seek help if they are affected by these issues e.g. peer mentoring or worry boxes. Pupils are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions. We ensure pupils develop an understanding of the importance of the Acceptable Use Policy and are encouraged to adopt safe and responsible use of ICT both within and outside school. Pupils are reminded of safe Internet use e.g. classroom displays, eSafety rules, acceptance of site policies when logging onto the school network/Virtual Leaning Environment.

6.2eSafety – Raising staff awareness

There is a planned programme of formal eSafety training for all staff to ensure they are regularly updated on their responsibilities as outlined in our school policy. The Head Teacher and ICT Subject Leader will provide advice/guidance or training to individuals as and when required e.g. eSafety champion or other nominated person. The members of staff delivering eSafety training received external eSafety training/updates from a county provider/CEOP. eSafety training ensures all staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites. All staff are expected to promote and model responsible use of ICT and digital resources. eSafety training is provided within an induction programme for all new staff to ensure that they fully understand both the school's eSafety Policy and Acceptable Use Policy. If regular updates on eSafety policy, Acceptable Use Policy, curriculum resources and general eSafety issues are discussed in staff meetings.

6.3eSafety – Raising parents/carers awareness

'Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it' (Bryon Report, 2008)

Our school offers regular opportunities for parents/carers and wider community to be informed about eSafety, including the benefits and risks of using various technologies. We do this through school newsletters, school website, moodle, other publications and promotion of external eSafety resources/online materials.

6.4eSafety – Raising Governors' awareness

Our school considers how Governors, particularly those with specific responsibilities for eSafety, ICT or child protection, are kept up to date. This may be through discussion at Governor meetings, attendance at Local Authority Training, CEOP or internal staff/parent meetings.

7 Standards and inspection

Since September 2009 there has been greater emphasis on monitoring safeguarding procedures throughout schools. We will know if our eSafety policy is having the desired effect by parent and pupil questionnaires, ICT lesson observations. eSafety incidents will be monitored, recorded and reviewed using an incident log whoch will be kept by the eSafety Champion. The eSafety Champion and the ICT Subject Leader are responsible for the monitoring, recoding and reviewing of incidents. The introduction of new technologies are always risk assessed and these assessments are included in the eSafety policy. Incidents and analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children. These patterns are addressed most effectively e.g. working with a specific group, class assemblies, reminders for parents. The monitoring and reporting of eSafety incidents contribute to the changes in policy and practice. Staff, parents/carers, pupils and governors are informed of changes to policy and practice in staff/governors meetings, newsletters and assemblies. The AUPs are reviewed and they do include reference to current trends and new technologies, they are reviewed yearly or when a new member of staff or pupil staff start school.