North Wolds Federation

E-Safety Policy

September 2015

- **The Federation e-safety officer is Miss Victoria Bottle**
- **The school internet breach log is kept in the behaviour file at each site.**

This policy should be read in conjunction with the safeguarding policy, acceptable use of ICT adult policy, Prevent risk assessment, acceptable use of ICT child policy and Twitter policy.

Introduction:
The use of digital technology is now an essential part of everyday life. 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.

Risks of Digital Technology
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. In more recent time use of digital technology, including social media, is a way used to radicalise children and young people.

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 have led to 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.

This policy and related guidance has been produced by LSCB, LCC and CfBT with other partner agencies in order to aid Lincolnshire schools in safeguarding children and young

people from risks and dangers present in the digital world . It has been modified by the North Wolds Federation to suit our settings.

Policy statement
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 should 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.

The objective of this policy is to state a minimum standard required by Lincolnshire County Council so that schools and other establishments in Lincolnshire can build their own requirements based on own needs.

E-Safety - what is e-safety?
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.

- 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.
- 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.

Schools have a **duty of care** to enable pupils to use on-line systems safely. Schools need to protect themselves 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.
Schools can help protect themselves 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, schools should be 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.

The purpose of Internet use in schools is to raise educational standards, to promote pupil achievements, to support the professional work of staff and to enhance the schools management information and business administration systems.

Teaching and Learning

Why the Internet and digital communications are important.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Internet use will enhance learning

- Access to world-wide educational resources.
- Educational and cultural exchanges between pupils world wide.
- Cultural, vocational, social and leisure use in libraries, clubs at home.
- Access to experts in many fields for pupils and staff.
- Staff professional development through national developments, educational materials and good curriculum practice.
- Communication with support services, professional associations and colleagues.

- Exchange of curriculum and administration data with LA and DfE. Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be shown how to publish and present information to a wider audience. The school must ensure that the use of Internet derived materials by staff and pupils complies with copyright laws.

Safe Use

- The school internet access will be designed expressly for pupils use and will include filtering appropriate to the age.
- Pupils will be taught what is acceptable and what is not and given clear objectives for internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the E Safety Officer.
- The use of mobile phones will not be permitted during school times.

Pupils will be taught how to evaluate Internet content

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed or any consequences on internet access.

- Pupils will be taught what to do if they experience material that they find uncomfortable or threatening.
- Pupils will be encouraged to question the validity and origins of information and look for alternative sources of information for comparison purposes.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.
- Wireless networks will be protected to the best of our ability from outside use
- Staff and students will change their passwords on a periodic basis
- Staff and students will log out of the system when not in use

Email

The government encourages the use of email as an essential means of communication and should be used appropriately.

- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in email communication.
- Access in school to external personal email accounts may be blocked.
- Email sent to an external organization should be written carefully before sending.
- The forwarding of chain letters is banned.
- Staff and children's email can be checked by staff.

The use of chat rooms.

- Pupils will not be allowed access to public chat rooms or unregulated chat rooms.
- Children should use only regulated educational chat environments. This use will always be supervised and the importance of chat room safety emphasised.
- Emerging technologies will be examined for educational benefits and a risk assessment will be carried out before use in school is allowed.

Published content and the school web site

- Staff or pupil personal contact information will not be published.
- The contact details given online should be the school office or school e-mail addresses.
- The Governing Body takes overall editorial responsibility to ensure that published content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified. Where possible we will use group photographs rather than full-face photos of individual children but there will be times when this is not the case, e.g. Star of the Week photographs and in the Picture Gallery.
- Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Use of Social Networking

- Social networking should not be used in school unless under strict monitoring arrangements.
- The exception to this is use of Twitter –See Twitter Policy.

Managing Filtering

Levels of access and supervision may vary according to the pupils' age and experience. Internet access must be appropriate for all members of the school community from the youngest pupil to teacher and administration staff.

- The school will work in partnership the LA and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- Regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported.

Policy Decisions

Authorising Internet access

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff leaving or the withdrawal of a pupil's access.

- At key stage one, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be informed that pupils will be provided with supervised Internet access and they will be asked to sign and return a consent form. Please see the sample form later in the document.

Assessing Risks

In common with other media such as magazines, books and videos, some materials available via the Internet are unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material.

- The use of computer systems without permission for the inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimize risks will be reviewed regularly.

Communications Policy

Introducing this policy to pupils

- Students will be made aware of e-safety rules and a programme of training in e-safety implemented into the curriculum.
- Students and parents will be informed that network, internet and ICT use will be monitored.
- A module on responsible Internet use will be included in the Independence Award.
- Parents will sign a consent for on admission for use of Internet. (See appendix B)

Staff and this policy

It is important that teachers and learning support assistants are confident to use the Internet in their work. This policy will only be effective if all staff subscribe to its values and methods.

- All staff have agreed the terms of this policy.
- All staff including teachers, supply staff, classroom assistants and support staff will be provided with this policy and its importance explained.
- Staff development in the safe and responsible Internet use and on school Internet policy will be provided as required.
- Staff must only use their own log in and password and not share theirs with others.
- Staff will sign a Information Systems code of conduct. (Appendix A)

Enlisting parents' and carers' support

Parents' and carers' attention will be drawn to this policy in newsletters, the school brochure and on the school Web site.

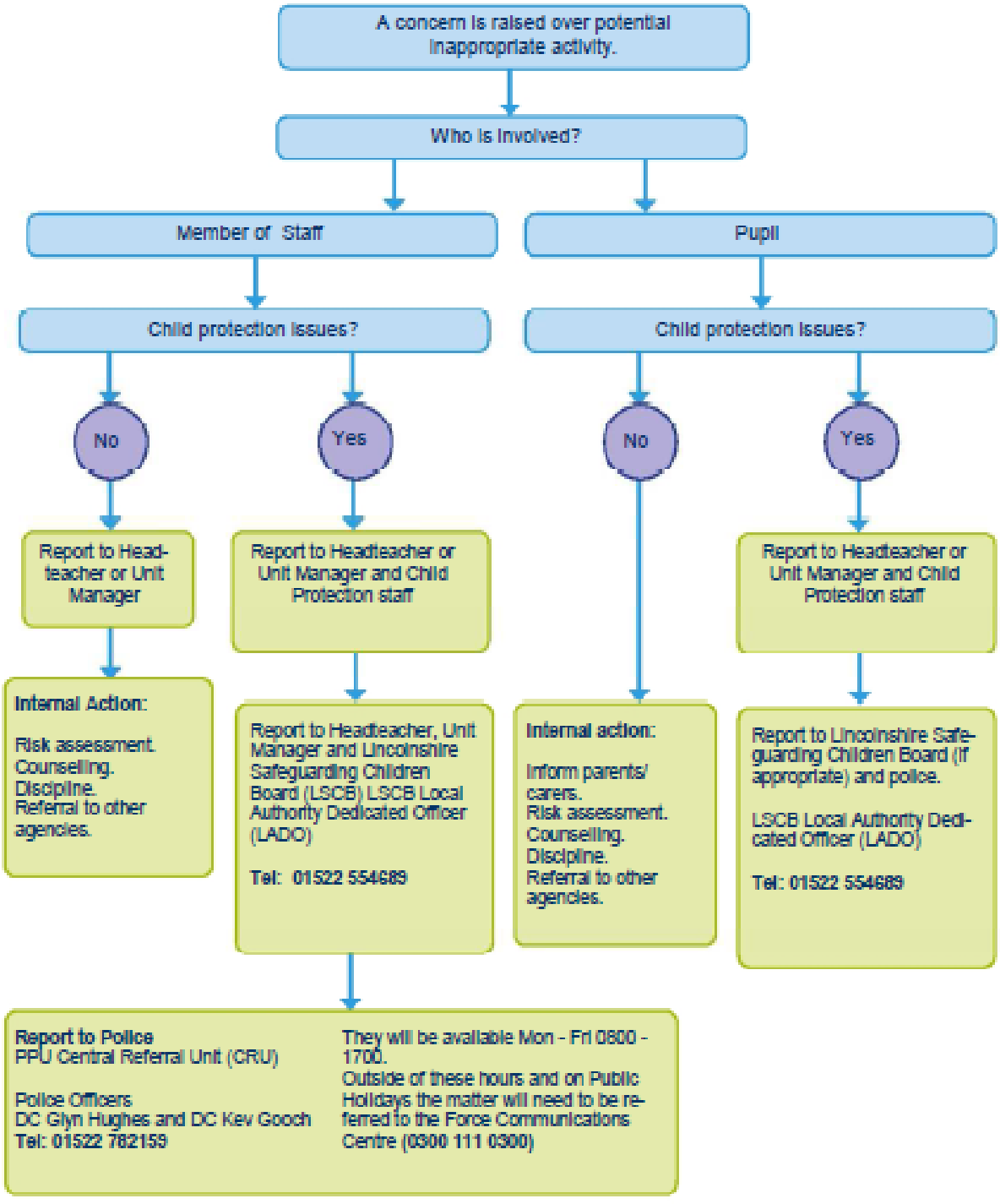
The PREVENT Agenda

The DFE document "The Prevent Duty" June 2015 makes clear the role schools play in keeping children safe from online extremism, radicalisation and grooming. As a school we have ensured that we have adequate filtering software in place that IT systems are checked on a weekly basis using the Securus software to identify and breaches of the firewall. All teachers have had Prevent training (05/15) and are therefore aware of the online risks of harm posed by the online activity of extremist and terrorist groups.

Inappropriate Activity.

In the case of inappropriate activity the following procedure, designed by Lincolnshire LSCB, will be used.

Inappropriate Activity flowchart



Appendix A

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that the laptop I use will be covered on my contents insurance for my home and car. If it is lost or stolen whilst in your possession and is not covered by my insurance, I will be liable for its replacement.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems, including social networking sites, may not be used for private purposes, without specific permission from the head teacher.
- I understand that it would be unprofessional to make negative or inappropriate comments concerning members of the school community or the management of the school in a public arena.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I understand that files created for educational purposes should not be deleted without the permission of the head teacher.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will respect confidentiality and not open or delete other people's files without their express permission.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials to check for unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …… Name: ……..

Date: ……

Appendix B

Market Rasen Church of England Primary School

PARENTAL CONSENT FORM

It is very important that we have your consent for various activities within school. This form will be kept on file and referred to throughout your child's time at Market Rasen Church of England Primary School. **Please complete all of the following statements, deleting as applicable.**

Should you wish to change your consent at any time in the future please let the office staff know so records can be updated.

- I consent/ do not consent to my child being photographed with name/without name at school events and on school visits under the terms of the schools photography policy.
- I consent/ do not consent to my child being photographed as part of a group and this photo being used on the school web site. I understand that my child's full name will not be used to identify him/her in the photo.
- I consent/ do not consent for my child's photograph to be published in local newspapers such as the Rasen Mail or Lincolnshire Echo with/without their name.
- I consent/ do not consent to my child watching PG certificate film clips in school, which have been approved for viewing by school staff.
- I consent/ do not consent to my child being fingerprinted for our school electronic library loaning system.
- I consent/ do not consent to my child using e-mail and the internet at school. I understand that pupils will be held accountable for their own actions. I also understand that some materials on the internet may be objectionable and I accept responsibility for setting standards for my child to follow, when selecting, sharing and exploring information.
- I consent/ do not consent to my child being issued with a ticket for Market Rasen Library (NB. If they do not already have one).
- I consent/ do not consent to my child taking part in visits around the local vicinity whilst a pupil at Market Rasen Church of England Primary School.

Child's Name _____

Parent/Guardian signature _____

Date _____

Useful websites:

www.ceop.gov.uk

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.iwf.org.uk

IWF (Internet Watch Foundation) provides the UK hotline to report criminal online content.

www.bbc.co.uk/cbbc/help/web/staysafe

BBC - a fantastic resource of e-safety information for the younger child.
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

Due to the rapidly changing world of technology this polciy will be reviewed annually.

Chair of Governors: Date

Head Teacher : Date