St Michael's C of E Primary School
e-Safety Policy

Updated 11.09.15 by CRG

POLICY STATEMENT

For clarity, the e-Safety policy uses the following terms unless otherwise stated:

Users - refers to staff, pupils, governing body, school volunteers (including students) and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents

Safeguarding is a serious matter; at St Michael's C of E Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety, is an area that is constantly evolving and as such this policy will be reviewed on a bi-annual basis or in response to an e-Safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the St Michael's C of E Primary School website; upon review all members of staff will sign as read and understood both the e-Safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Pupil Acceptable Use Policy will be sent home with children at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, pupils will be permitted access to school technology including the Internet.

Headteacher Name:	Mr P Fox	Signed:…….
Chair of Governors:	Mr I Roscoe	Signed: …….
Review Date:	Sept 2016	Next Review:…….

POLICY GOVERNANCE (ROLES & RESPONSIBILITIES)

Governing Body

The governing body will:

- Review this policy annually and in response to any e-Safety incident to ensure that the policy is up-to-date, to ensure that it covers all aspects of technology use within the school, to ensure e-Safety incidents were appropriately dealt with and to ensure the policy was effective in managing those incidents.

- Appoint one governor to have overall responsibility for the governance of e-Safety at the school who will:
  - Keep up-to-date with emerging risks and threats through technology use.
  - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-Safety within our school. The day-to-day management of this will be delegated to two members of staff, the e-Safety Officers, as indicated below.

The Headteacher will ensure that:

- e-Safety training throughout the school is planned and up-to-date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body.
- The designated e-Safety Officers have had appropriate CPD in order to undertake the day to day duties.
- All e-Safety incidents are dealt with promptly and appropriately and retain responsibility for the e-Safety incident log; ensure staff know what to report and ensure the appropriate audit trail.

e-Safety Officers

The day-to-day duty of e-Safety Officer is devolved to E. Wood (child protection officer) and C. Royston-German (Computing Coordinator).

The e-Safety Officers will:

- Keep up to date with the latest risks to children whilst using technology; be familiar with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Work with the Headteacher to advise the governing body on all e-Safety matters.
- Engage with parents and the school community on e-Safety matters
- Liaise with the local authority, IT technical support and other agencies as required.
- Ensure any technical e-Safety measures in school (e.g. Internet filtering software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make themselves aware of any reporting function with technical e-Safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Operating system updates are regularly monitored and devices updated as appropriate.
    - Any e-Safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-Safety officers and Headteacher.
    - Passwords are applied correctly to all users regardless of age and are changed annually/when required. Passwords for staff will be a minimum of 8 characters.
    - Passwords for pupils can be shorter to make them age-appropriate.
    - The IT System Administrator password is to be changed on a monthly (30 day) basis.

Signed……. (Education Lincs)

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any e-Safety incident is reported to the Headteacher and e-Safety Officers (and an e-Safety Incident report is made). If you are unsure the matter is to be raised with the e-Safety Officers or the Headteacher to make a decision.
- The reporting flowcharts contained within this e-Safety policy are fully understood.

All Pupils

The boundaries of use of ICT equipment and services in this school are given in the Pupil Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

e-Safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly all pupils will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through school newsletters and the school website, the school will keep parents up to date with new and emerging e-Safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the Pupil Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Health & Safety Committee

e-Safety is discussed under the Safeguarding committee and the governors meet five times a year.

- Governors will be advised on changes to the e-Safety policy.
- Governors will establish the effectiveness (or not) of e-Safety training and awareness in the school.

TECHNOLOGY

St Michael's C of E Primary School uses a range of devices including PCs, laptops, iPads, MacBooks and Nintendo DS consoles. In order to safeguard the pupils and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – The school uses a Meraki MX security appliance which is CIPA-compliant (Children's Internet Protection Act). This prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Computing Coordinator, e-Safety Officers, the Headteacher and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher. St. Michael's school has an appropriate level of filtering on accessing the internet in school to ensure that both staff and children are safe from accessing radical and extremist material whilst using networks and devices in school.

Email Filtering – The school uses the Gmail system and Google has comprehensive virus protection, Spam filtering & Message Centre and quarantine summary. This helps prevent any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.
(Note: Encryption does not mean password protected.)

Passwords – all staff and pupils will be unable to access any device without a unique username and password. Staff and pupil passwords will change if there has been a compromise. The ICT Coordinator and IT Support will be responsible for ensuring that passwords are changed. Please note that the Nintendo DS consoles cannot be password protected. As we are now using Google Drive and sensitive data is stored online, it is imperative that Gmail passwords contain a mixture of capital and lower case letters, numbers and punctuation. There are NOT to be written down or shared with ANYONE.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated whenever our ICT technician visits (currently every other week but after April this will be once a week). IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns.

SAFE USE

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-Safety and the staff Acceptable Use Policy; pupils upon receiving parental signature and returning their acceptance of the Pupil Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted. Older pupils are permitted to use the school email system, and as such will be given their own email address.

Photos and videos –All parents must sign a photo/video/social media release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

Social Networking – there are many social networking services available; St Michael's C of E Primary School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within St Michael's C of E Primary School and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the e-Safety Officers who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff in school.
- Twitter – used by the school as a broadcast service (see below).
- Facebook - used by the school as a broadcast service (see below).

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permission slips must be consulted before any image or video of any child is uploaded.
- There is to be no identification of pupils using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed as soon as possible.

Incidents - Any e-Safety incident is to be brought to the immediate attention of the e-Safety Officers, and the Headteacher. The e-Safety Officers and Headteacher will assist in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, St Michael's C of E Primary School will have an annual programme of training which is suitable to the audience.

e-Safety for pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupils' learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The e-Safety Officers are responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

For the academic year 2014/15, the e-Safety training will be a whole school and governor CPD session led by Alan McKenzie. For members of teaching staff there will be updates throughout the year (during staff meeting time) from the e-Safety academy.

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the e-Safety Policy. Once you have read and understood both you must sign this policy sheet.

Internet access - You must not intentionally 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. Inadvertent access must be treated as an e-Safety incident, reported to the e-Safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the e-Safety policy only. Staff using social networking for personal use should never undermine or bring into disrepute the school, its staff, parents or children.

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pendrive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device. Please contact IT support if you require assistance with this.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload on to any internet site or service images or videos of other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings). Photographs and videos of children should only be taken on school cameras/iPads and never taken offsite. Personal cameras/iPads/mobile phones should not be used under any circumstances for photographs or videos.

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the e-Safety Officers if required.

Viruses and other malware - any virus outbreaks are to be reported to the Mouchel Helpdesk and Education Lincs as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

e-Safety – is a safeguarding issue and therefore is the responsibility of everyone. As such you will promote positive e-Safety messages in all use of ICT whether you are with other members of staff or with students.

iPads – staff are not to log on to the iTunes Store using personal iTunes accounts. No app purchases/downloads should be made without the consent of the subject coordinator (CRG) or head teacher (PF).

NAME : ……

SIGNATURE : …… DATE : ……

Acceptable Use Policy – Pupils

St Michael's C of E Primary School's Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online ; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher or an adult I trust if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Parent): …… on behalf of …… (pupil)

Date: ……..

Sample Letter to Parents:

Dear Parent/Guardian

Use of the Internet in school is a vital part of the education of your child. Our school makes extensive use of the Internet in order to enhance their learning and provide facilities for research, collaboration and communication.

You will be aware that the Internet is host to a great many inappropriate websites, and as such we will ensure as far as possible that your child is unable to access sites such as this. We are able to do this using advanced software known as an Internet filter. This filter categorizes websites in accordance with their content; the school allows or denies these categories dependent upon the age of the child.

The software also allows us to monitor Internet use; the Internet filter keeps logs of which user has accessed what Internet sites, and when. Security and safeguarding of your child are of the utmost importance in our school; in order to ensure that there have been no attempts of inappropriate Internet activity we may occasionally monitor these logs. If we believe there has been questionable activity involving your child we will inform you of the circumstances.

At the beginning of each school year we explain the importance of Internet filtering to your child. Furthermore we explain that there has to be a balance of privacy and safety; we also inform them that we can monitor their activity. All children are given the opportunity to ask questions and give their viewpoint. We would like to extend that opportunity to you also; if you have any questions or concerns please contact 'enquiries@st-michaels.lincs.sch.uk'.

Yours Sincerely

P Fox
Head Teacher

I have read this letter and understand that my child's Internet access could be monitored to ensure that there is no illegal or inappropriate activity by any user of the school network. I acknowledge that this has been explained to my child and that he/she has had the opportunity to voice their opinion, and to ask questions.

Name of Parent/Guardian –

Name of Child –

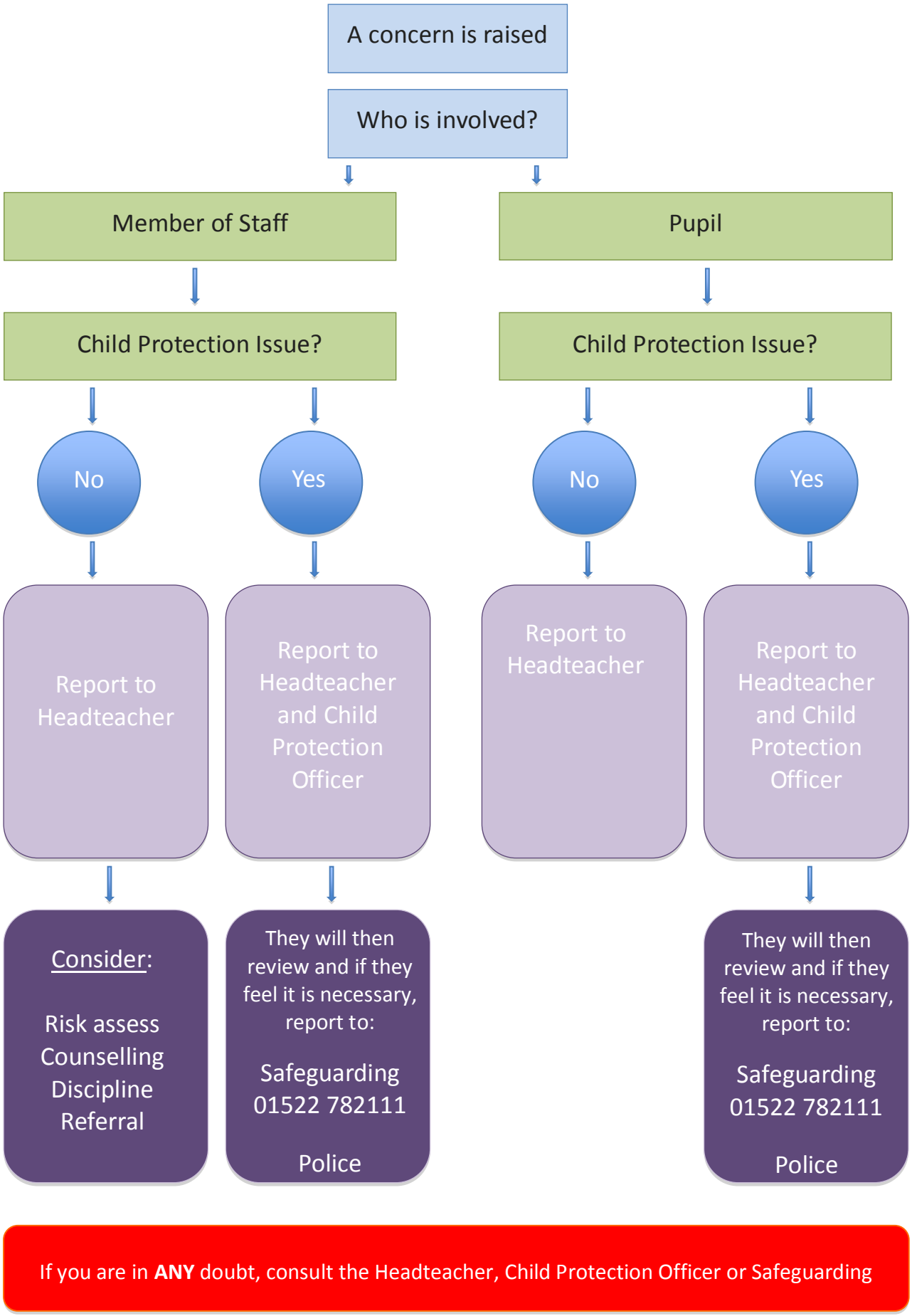
Signature - Date

St Michael's C of E Primary School e-Safety Incident Log

Reported By: *(name of staff member)*	**Reported To:** *(e.g. Head Teacher, e-Safety Officers)*
When:	**When:**
Where did the incident originate? *(e.g. home or school)*	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)	
Review Date:	
Result of Review:	

Signature (Headteacher)		**Date:**	
Signature (Governor)		**Date:**	

Inappropriate Activity Flowchart



If you are in **ANY** doubt, consult the Headteacher, Child Protection Officer or Safeguarding

Illegal Activity Flowchart