Online Safety Policy

St Michael & St John's RC Primary

Date Created: February 2016
Updated: June 2018

Contents

Policy Creation and Review

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

Emma Jackson, Zoe Mabbott and St Michael & St John's School Council members

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

Policy Created - Date: **February 2016**
Policy Updated – Date: **June 2018**

Intended Policy Review - Date: **June 2019**

The implementation of this policy will be monitored by:
Emma Jackson

This policy will be reviewed as appropriate by:

Approved by …….....…….. (Headteacher)

Date: ……..…….....

Approved by …….....…….. (Governor)

Date: ……..…….....

This policy should be read in conjunction with the School Mission Statement and the Behaviour Policy, Safeguarding and Child Protection Policy, Anti bullying policy and Visitor Policy.

1. Introduction

Our online Safety Policy has been written by the school, building on the Kent online Safety Policy with advice from Lancashire Safeguarding Children Board online Safety Group, SWGfL, Kent NGfL, Plymouth early years team and government guidance.

This online Safety policy should be updated regularly, at least on an annual basis, or to reflect changing circumstances, purchase of new equipment or incidents within the school. Our policy is integrated with other relevant school policies, initiatives and documents, for example EYFS framework, behaviour, safeguarding and anti- bullying policies.

In a recent Ofsted document (February 2013 - Information Communication Technology (ICT) survey visits), one of the criteria listed for ICT to be regarded as good/outstanding, is that online Safety is a priority across all areas of the school.

Online Safety will naturally tend to focus on reducing the potential risks; however it should equally promote the benefits to be gained from the opportunities afforded through use of technology.

2. Our school's vision for Online Safety

At St Michael & St. John's Roman Catholic Primary School we aim to secure the best for all pupils as individuals. We strive for them to be the best that they can be. This approach means that every effort is made to promote a positive school climate that recognises the rights of all pupils. These rights include the right to stay safe at all times, including when using technology both in school and out. Online Safety is at the heart of all our teachings in order to enable and encourage all those involved with school to have a safer use of technology.

We aim to provide a diverse, balanced and relevant approach to the use of technology. The children are encouraged to maximise the benefits and opportunities that technology has to offer in a safe and enabling environment.

St Michael and St John's school ensures that children learn in an environment where security measures are balanced appropriately with the need to learn effectively, whilst also equipping the children with the skills and knowledge to use technology appropriately and responsibly.

We teach how to recognise the risks associated with technology and how to deal with them, both within school and outside the school environment. All users in the school community understand the need for an Online Safety policy.

3. The school's Online Safety Champion

St Michael and St John's school has appointed an online safety Champion to be the main point of contact for online safety related issues and incidents. Mrs Jackson has been appointed this role due to the inter-related roles of online safety Coordinator, ICT Coordinator and DSL (Designated Safeguarding Lead).

The role of the online safety Champion includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school's online safety 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 online safety incident occur.
- Ensuring an online safety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with online safety issues and guidance through liaison with the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging online safety advice/training for staff, parents/carers and governors.
- Ensuring the Headteacher, SLT, staff, children 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.

The online safety Policy refers to this nominated person so that all users are aware of the main contact in event of queries or incidents.

4. Security and data management

ICT security is a complex subject that involves all technology users in the school, dealing with issues regarding the collection and storage of data through to the physical security of equipment. The *Lancashire ICT Security Framework* (published 2005) has been consulted to ensure that procedures are in place to ensure data, in its many forms, is kept secure within the school.

In line with the requirements of the Data Protection Act (1998), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data is:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection.

All data in our school is kept secure and staff informed of what they can or can't do with data through the online safety Policy and statements in the Acceptable Use Policy (AUP).

The school bursar, under direction from the Headteacher has the responsibility for managing information and allows staff some access to personal data whilst showing understanding of their legal responsibilities.

St Michael & St John's school ensures that data is appropriately managed both within and outside the school environment as all staff, Governors, supply teachers etc. adhere to the Acceptable Use Policy relevant to them. Also, the above named groups use secure email for contact regarding school matters, these emails are managed by Lancashire Local Authority and are treated with confidence ensuring no confidential information can be accessed. Staff are aware that they should only use approved means to access, store and dispose of confidential data. Staff are aware of the dangers of unsecured wireless access at home when accessing school data remotely. In line with new GDPR (General Data Protection Regulation) Children's profiles, names and/or information pertaining to the school are not stored using 'cloud' storage facilities e.g. Dropbox/ SkyDrive, all teachers have been given an encrypted pen drive for movement of information between home and school if needed. The use of Junior Librarian in school does not include Biometric information as children use a barcode scanner for borrowing books. Their names are the only information held in the system and are only accessible through the school intranet.

Teachers are provided with a school laptop (mobile device), these are password protected and confidential information is stored securely on these. Personal devices are not used to access data on school systems e.g. downloading e-mail or files. The school back up all data on the Bursar's system at the end of every day to ensure the risk of data lost is addressed and managed.

Data is backed up on the bursar's system every night and this information is stored securely in accordance with recommended guidance from Lancashire Local Authority.

5. Use of mobile devices

School use of mobile devices, including laptops, tablets, mobile phones, cameras and games consoles is becoming more commonplace. Whilst these can provide a flexible solution and offer a range of exciting opportunities to extend children's learning, their use poses challenges in terms of online safety. Many of these devices integrate functionality to take images, access the Internet and engage users in various methods of external communication.

St Michael & St John's school provides some devices e.g. iPads for use in class but do not allow staff (or children) to bring personal devices into school to use as resources for teaching and learning,
The EYFS framework: Section 3.4 (2012) states that

"....Safeguarding policy and procedures must include an explanation of the action to be taken in the event of an allegation being made against a member of staff, and cover the use of mobile phones and cameras in the setting."

Our school has considered what is acceptable with regard to the use of mobile phones and cameras. This is that staff do not use their personal mobile devices (including phones) when the children are within the environment, they are to be used (unless specific permission has been given by the Headteacher) during breaks or lunch or out of lesson times. In the event that a personal mobile device needs to be accessed during the school day this should be done so in a room/ environment where children are not present. These personal devices should not be used for photographs or storage of school data. In response to the requirements of the EYFS framework, and to avoid confusion or misinterpretation, our school has implemented procedures with respect to mobile devices across the whole school.

Mobile phones

Mobile phones can present a variety of challenges if not used appropriately and we have definite and clear boundaries for their use. They are valuable items that can be lost, stolen or damaged in the school environment and could also be considered as distracting or intrusive in a teaching or learning situation. However, staff and parents may equally have valid reasons why mobile phones should be readily

available. Rules for mobile phone use are (including those mentioned above) children needing a mobile phone for walking to/ from school (with permission from parents) should hand it to the school office for safe keeping until the end of the school day. Staff mobile phones should be on silent during the school day. Staff and visitors can be contacted in the event of emergency via the school office. Images, video or audio must not be recorded on a personal mobile phone without specific authorisation from the Headteacher.

Users are allowed to access the Internet via personal mobile phones (during their own time) using the school's secure wi- fi connection after getting the password from the school office. There is a 'work' device for staff to use, for example, whilst outside the main buildings or on trips, the use of this is subject to the Acceptable Use Policy and should be used in an emergency situation. School data, photos, video/ audio should not be stored on this device. It is the responsibility of the last person to use the device to ensure it is always ready for use e.g. fully charged and 'in credit' (the school bursar needs informing regarding 'credit'). Visitors, including parents are made aware of our rules for acceptable use of a mobile phone through the publication of the online safety policy on the school website.

Staff are aware of the potential for mobile phones to be used for cyberbullying through training and anti- bullying activities during anti- bullying week in November of each year as well as online safety week activities each February. Cyberbullying prevention activities are completed during these two designated weeks in November and February. The reporting of cyberbullying is to be done through the online safety champion who will then follow these steps;

- Ask the child not to reply
- Save the evidence
- Block the bullies
- Explain the severity to the bully
- Contact parents of involved parties
- Inform the website involved e.g. Facebook, twitter or Youtube
- Get advice from Lancashire Local Authority
- Contact police where applicable

Other mobile devices

The school allows use of personal mobile devices during their own time in school by adults in line with the Acceptable Use Policy. The adult is allowed access to the internet using the school's secure wi- fi connection after getting the password from the school office; this will then mean the mobile device is subject to the same filters as school devices. The device owners will be aware of their responsibility to ensure all content on these devices is legal and appropriate for a school setting through the Acceptable Use Policy. The owners are also aware that the school cannot be held liable e.g. for any damage or theft of personal devices. Devices should be 'virus checked' (if applicable) before use on school systems by the owner.

Physical security of school based devices is through the devices being locked away at night, classrooms are locked when applicable as well as the school monitored alarm system being in use.

Tablet devices:

Copyright legislation is compliant when purchasing content through discussion with computer technician and/or advice from content suppliers. Content is transferred between devices under direction of the technician and via the use of 'cloud' storage linked to secure email accounts provided by Lancashire Local Authority. Users are aware of any 'sanctions' for misuse of mobile devices through the Acceptable Use Policy.

6. Use of digital media (cameras and recording devices)

Photographs and videos of children and adults may be considered as personal data in terms of The Data Protection Act (1998). To ensure all users are informed about the risks surrounding taking, using, sharing, publishing and distributing digital media, we have decided on the following points for inclusion in our online safety Policy.

Consent and Purpose

Written consent from parents for photographs of their children to be taken or used is covered through the image consent form in the appendices, there is also a consent form for the use of adults employed in the setting for their photographs to be taken or used. When consent is gained it is made clear how photographs can/ cannot be used (including the use of external photographers or involvement of 3rd parties.)

The consent includes permission to store / use images once a child has left the school e.g. for brochures, displays etc with parents being informed of the timescale for which images will be retained. This permission is obtained annually and parents are requested to inform the school of any change in circumstances that may necessitate removal of permission, enabling the online safety champion to action removal of images.

Parents are informed of the purposes for which images may be taken and used e.g. displays, website, brochures, learning journeys and portfolios, press / other external media through the image consent form.

Some images are displayed in public areas e.g. the entrance hall and office area, with the purpose of these being the different roles and responsibilities of the children e.g. sports clubs, school council members, pupil chaplains etc. and children volunteer/ are elected for these roles.

The consent form covers the use of children's images to be included in portfolios maintained by trainees / students not directly employed by the setting; the form also covers the use of images in group situations such as those used in children's profiles in the EYFS setting. Due to the image consent form being updated annually this ensures only current images are used, i.e. not children / adults who have left the setting.

The press have special permissions in terms of Data Protection and may wish to name individual children to accompany a photograph and at times, the media may publish an image in their online publication which may offer facilities for the 'public' to add comments in relation to a story or image. These can potentially invite negative as well as positive comments. These are explained to parents on the image consent form.

All adults working in the setting are kept informed of any children / other adults whose photographs must not be taken through details being kept in a list by the bursar, and adults must request this information prior to taking/ using images of children/ adults.

Taking Photographs / Video

All staff are authorised to take images as long as they have signed the AUP which states that any images/ videos taken should only be using school equipment unless specific permission is given by the headteacher.

When taking photographs/ video the rights of an individual to refuse to be photographed is respected and it is ensured that the photograph doesn't show children who are distressed, injured or in context that could be

embarrassing or misinterpreted. Every effort is made to ensure certain children are not continually favoured when taking images. Subjects are appropriately dressed and not participating in activities that could be misinterpreted including when considering the angle of shots for children engaged in P.E. activities. Certain areas are classed as 'off limits' for taking photographs, e.g. toilets, cubicles etc. Close up shots are avoided as these may be considered intrusive. Shots should preferably include a background context and show children in group situations.

Parents Taking Photographs / Videos

Under the Data Protection Act (1998), parents are entitled to take photographs of *their own* children on the provision that the images are for ***their own*** use, e.g. at a school production. Including other children or other purpose could constitute a potential breach of Data Protection legislation. Through the image consent form parents are informed that they should only take photographs/ videos of their own children (special events such as performances are covered separately using the 'consent form for images at a special event') parents are reminded of this at the beginning of each year when signing the consent form and the special event form.

Storage of Photographs / Video

Images are stored securely on the school computers and are not stored on portable devices, USB memory sticks or in 'cloud' storage. We do not allow images to be stored outside of the school equipment unless it is stored by the school photography company and is in line with the Data Protection Act (1998). Staff are not allowed to store images on personal equipment e.g. tablets, laptops or USB storage devices. Only staff have access to images and videos stored on school equipment due to the images being stored in staff only, password protected domains.

It is the responsibility of the online safety champion for deleting photographs / video or disposing printed copies (e.g. by shredding) once the purpose for the image has lapsed or should a parent withdraw permission. If photographs are 'sent' electronically, this is done using the school staff allocated emails which are hosted by Lancashire local authority.

Publication of photographs/ videos

Publication of images is only done through the secure school website which is hosted by Lancashire local authority and the images are of children whose parents have given permission using the image consent form.

When publishing photographs, care is taken over the choice of images to ensure that individual children / adults cannot be identified or their image made available for downloading or misuse, e.g. through the use of low definition images that will not magnify effectively. Full names and/ or other personal information does not accompany published images.

When publishing images

Children's images are not displayed on insecure sites e.g. Social Networking Sites by staff as they have signed the AUP, parents are also asked to sign the 'image consent form' which refers to the storage and use of images on Social Networking Sites.

Staff are aware that full names and personal details will not be used on any digital media, particularly in association with photographs. They also recognise the risks associated with publishing images, particularly in relation to use of personal Social Network sites. It is also recognised that staff ensure their personal profiles are secured and do not display content that is detrimental to their own professional status or could bring the

school into disrepute.

The media, 3rd parties and copyright

3rd parties are supervised whilst in the school and are able to comply with the Data Protection requirements in terms of taking, storage and transfer of images. The school owns the copyright for images taken by a 3rd party. If uploading images to a 3rd party website, e.g. for printing or creating calendars, cards etc. it is ensured that the person uploading reads the terms and conditions of the website. Permission could unknowingly be granted for the site's host license to modify, copy or redistribute images without further consent. The site may also be advertised for 'personal use' only therefore using for business purposes would be a breach of the terms and conditions.

CCTV, video conferencing, VOIP and webcams

St Michael and St John's RC Primary School does not use CCTV, video conferencing, VOIP or webcams.

7. Communications technologies

Schools use a variety of communication technologies and need to be aware of the benefits and associated risks. New technologies are risk assessed against the potential benefits to learning and teaching before being employed throughout the school. This is done before multiple devices are purchased. As new technologies are introduced, the online safety Policy is updated and all users are made aware of the changes.

E Mail

The following statements reflect good practice in the use of email;

- All users have an Office365 email which any school information is sent via, these are the recommended email by Lancashire.
- Staff have permission to access personal email accounts on school equipment provided it is in accordance with the AUP (in appendix).
- The junior children have email accounts which have been set up using the Office365 service and these have been set in such a way that the children cannot be identified by them e.g. j.smith@ssmj.lancs.sch.uk
- Staff and children are made aware that only official email addresses should be used for contact.
- 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 'One Connect'
- All users are aware of the risks involved in accessing content including SPAM, phishing, unsuitable materials and viruses from external email accounts e.g. Hotmail or Gmail in school.
- All users are aware that the email is covered by the Data Protection Act (2018) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- All users are aware that email may be monitored at any time in accordance with the Acceptable Use Policy.
- The content of children's email accounts is monitored by both the online safety champion and parents of each child.
- Users should report any content that makes them feel uncomfortable, is offensive, threatening or bullying in any way to the online safety champion.
- Users are aware they should not open attachments that they suspect may contain illegal content as they could inadvertently be committing a criminal act.

- The school has a disclaimer at the bottom of all email addresses.

Social Network sites

Social Network sites allow users to be part of a virtual community. Current popular examples of these sites are Facebook, Twitter, Instagram and Snapchat, also some interactive computers such as Xbox and Wii. These sites provide users with simple tools to create a profile or page including basic information about themselves, photographs, and possibly a blog or comments. As a user on a Social Network site, you may have access to view other users' content, send messages and leave unmediated comments. Many Social Network sites are blocked by default through filtering systems used in school.

Although use of Social Network tends towards a personal basis outside of school environment, their use as a tool for communicating with parents is becoming more commonplace in primary schools. Guidance for personal publishing sites is included as part of staff induction, discussed regularly and outlined in the staff Acceptable Use Policy – along with sanctions for inappropriate use.

Whatever methods of communication are used, individuals should always conduct themselves in a professional manner. If content is made available on the web it is available for everyone to see and potentially remains there forever. Please also refer to the school's social media policy.

All staff are aware of the following points:

- The content on Social Network sites may be unmediated and inappropriate for certain audiences.
- If a Social Network site is used personally, details must not be shared with children and privacy settings be reviewed regularly to ensure information is not shared automatically with a wider audience than intended.
- They must not give personal contact details to pupils or parents/ carers including mobile telephone numbers, details of any blogs or personal websites.
- The content posted online should not:

  - bring the school into disrepute
  - lead to valid parental complaints
  - be deemed as derogatory towards the school and/ or its employees
  - be deemed as derogatory towards pupils and/or parents and carers
  - bring into question their appropriateness to work with children and young people.

- Adults must not communicate with children using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted. Online Communications with parents, past pupils or siblings of pupils, especially if under the age of 18 should be discouraged.
- Children must not be added as 'friends' on any Social Network site.

The school has also considered the advice provided for parents in terms of their use of Social Networking sites and how the school will respond to identified issues. Common concerns that have had consideration include:

- Posting inappropriate comments about staff or children that could be construed as instances of cyberbullying.
- Posting of images of children or adults on profiles without permission of the individuals involved, especially if the photographs contain children other than their own.

Websites and other online publications

Information posted online is readily available for anyone to see and thus form an opinion about the school. From September 2012, the School Information (England) (Amendment) Regulations 2012 specified that certain up to date information must be made available on a school's website.
At St Michael and St John's RC Primary school we ensure that:

- The school website is effective in communicating online safety messages to parents and carers as this policy is on the school website and there are also links to useful online safety websites.
- Everybody in the school is made aware of the guidance for the use of digital media on the website/ online publication.
- Everybody in the school is aware of the guidance regarding the inclusion of personal information on the website/ online publication.
- Staff have limited access to edit online publications and ensure the content is relevant and current with the headteacher, web editor and web host having overall responsibility for what appears on the website.
- There is no content that needs to be hidden behind a password protected area.
- 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.

8. Infrastructure and technology

The school ensures that the infrastructure/ network is as safe and secure as possible. The school subscribe to the Lancashire Grid for learning/ CLEO Broadband Service, therefore the internet content filtering is provided by default. It is important that the filtering service offers a 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 and this is installed on computers in school and then configured to receive regular updates.

Children's access

The children are supervised when accessing school equipment and online materials (e.g. working with a trusted adult). The children have limited access to the school systems through class logins, this access is restricted to certain areas of the network. Children must never be allowed to access school computers/ internet unsupervised in school.

Adult access

Staff have logins where most of the school systems are available to them, with the others have a hierarchical level of access increasing in the order shown - ICT coordinator, head and ICT technician (who has full access).

Passwords

All staff are aware of the guidelines in the Lancashire ICT Security Framework for Schools. (This is available at https://www.lancsngfl.ac.uk/onlinesafety/download/file/ICT%20Security%20Framework%20Policy_full%202005%20June10.pdf website). All users of the school network have a secure username and

password. The administrator password for the school network is available for the headteacher and ICT Coordinator and is kept in a safe place. Staff and children are reminded of the importance of keeping passwords secure.

Software/ hardware

School have legal ownership of all software (including apps on tablet devices), and an up to date record of appropriate licenses for all software is kept. The Bursar, ICT Coordinator and ICT Technician are responsible for maintaining this. School regularly audit equipment and software with installation of the software being under control of the headteacher and technician.

Managing the network and technical support

Servers, wireless systems and cabling are securely located and physical access is restricted. All wireless devices have security enabled and these devices are only accessible through a secure password available from the school bursar. Relevant access settings have been restricted on tablet devices e.g. downloading of apps or 'in-app' purchases. The headteacher and ICT technician are responsible for managing the security of the school network through regular visits from the technician enabling him to update the system with critical software updates/ patches.

Users (staff, children and guests) have clearly defined access rights to the school network through the usernames and passwords, with permissions assigned by the headteacher and ICT Coordinator. Staff and children are reminded to lock or log out of a school system when the computer/ digital device is left unattended. Users are not allowed to download executable files or install software. The headtecher and ICT technician are responsibility for assessing and installing new software. Users report any suspicion or evidnce of a breach of security to the online safety champion.

The school's guidance on using removable storage devices on school equipment is that children must seek permission from their teacher before being allowed to use these devices and staff can use them in accordance with the Acceptable Use Policy. Network monitoring takes place in accordance with the Data Protection Act (2018). All internal/ external technical support providers are aware of the schools requirements/ standards regarding online safety. The ICT Coordinator and headteacher are responsible for liaising with / managing the technical support staff.

Filtering and virus protection

The school filtering is managed by Lancashire Grid for learning filtering service. Procedures are in place to ensure that ALL equipment including school laptops used at home are regularly updated with the most recent version of virus protection software used in school as these updates are completed automatically every time the internet is accessed.

9. Dealing with incidents

The school is aware of the types of incident that may occur and how these will be dealt with. An incident log (see Appendix) is completed to record and monitor offences. This is audited on a regular basis by the online safety champion or other designated member of the Senior Leadership Team.

Illegal offences

Any suspected illegal material or activity is brought to the immediate attention of the headteacher who refers this to external authorities e.g. Police, CEOP, Internet Watch Foundation (IWF). The school will never personally investigate, interfere with or share evidence as we may be inadvertently committing an illegal offence. Correct procedures are followed when preserving evidence to protect those investigating the incident (see Appendix). Potential illegal content should be reported to the Internet Watch Foundation (https://www.iwf.org.uk/). 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
- Incitement to racial hatred

More details regarding these categories can be found on the IWF website https://www.iwf.org.uk/

Inappropriate use

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and actions are proportionate to the offence. The school have decided what constitutes inappropriate use and the sanctions to be applied. Some examples of inappropriate incidents are listed below with suggested sanctions.

Incident	Procedure and sanctions
Accidental access to inappropriate materials.	• Minimise the webpage/turn the monitor off/click the 'Hector Protector' button. • Tell a trusted adult. • Enter the details in the Incident Log and report to LGfL filtering services if necessary. • Persistent 'accidental' offenders may need further disciplinary action.
Using other people's logins and passwords maliciously. Deliberate searching for inappropriate materials. Bringing inappropriate electronic files from home. Using chats and forums in an inappropriate way.	• Inform SLT or designated online safety Champion. • Enter the details in the Incident Log. • Additional awareness raising of online safety issues and the AUP with individual child/class. • More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. • Consider parent/carer involvement. • If this is a member staff then the school discipline policy may be applicable.

- Mrs Mabbott and Mrs Jackson have responsibility for dealing with online safety incidents in their roles of Child Protection Officer, online safety Champion, ICT Coordinator.
- All staff are made aware of the different types of online safety incident and how to respond appropriately e.g. illegal or inappropriate.
- Procedures to deal with online safety incidents are followed using the example provided by Lancashire Grid for learning (Appendix 12), children are informed of these procedures through the display of Appendix 12 in the ICT suite.
- These incidents are logged on the 'incident log' (Appendix 11)
- These incidents are monitored by Mrs Mabbott, Mrs Jackson and the chair of Governors on a termly basis; this enables response and prevention of recurrence of incidents.
- External agencies and parents/ carers are involved in accordance with the guidance given in Appendix 12.

The school's Behaviour Policy outlines policy and procedures relating to the powers of 'search' referred to in the Education Act (2011). Items 'banned' in school include for example electronic devices such as mobile phones (unless staff have given permission for individual reasons).

10. Acceptable Use Policy (AUP)

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

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

A set of AUPs are provided in the appendices. The school AUPs:

- Reflect the content of the school's wider online safety Policy.
- Are regularly reviewed and updated.
- Are regularly communicated to all users, particularly when changes are made to the online safety Policy/ AUP.
- Are understood by each individual user and relevant to their setting and role/ responsibilities.
- Outline/ summarise acceptable and unacceptable behavior 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 is enforced.
- Outline sanctions for unacceptable use and make all users aware of the sanctions.
- Stress the importance of online safety education and its practical implementation.
- Highlight the importance of parents/ carers reading and discussing the content of the AUP with their child.

11. Education and training

In 21st Century society, both adults and children need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that children are taught to use technology responsibly, securely and safely, being able to recognize potential risks and knowing how to respond. They should, for example, be able to communicate safely and respectfully online, be aware of the necessity to keep personal information private, be taught how to search effectively and be discerning in their evaluation of digital content and be aware of the need to respect copyright and Intellectual Property rights.

Digital Resilience

Using guidance from The UK Council for Child Internet Safety (UKCCIS) the school has adopted a digital resilience section to their online safety teaching. These are split into key themes which are:

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, wellbeing and lifestyle
- Privacy and security, and
- Copyright and ownership

The three main areas of online safety risk (as mentioned by OFSTED, 2013) that the school is aware of and have considered are:

Area of risk	Example of risk
Content: Children need to be taught that not all content is appropriate or from a reliable source.	• Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse. • Lifestyle websites, for example pro-anorexia/self-harm/suicide sites. • Hate sites. • Content validation: how to check authenticity and accuracy of online content.
Contact: Children 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 in all forms • Identity theft (including 'frape' - hacking Facebook profiles) and sharing passwords.
Conduct: Children need to be made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others.	• Privacy issues, including disclosure of personal information, digital footprint and online reputation • Health and well-being - amount of time spent online (internet or gaming). • Sexting (sending and receiving of personally intimate images).

	• Copyright (little care or consideration for intellectual property and ownership – such as music and film).

(Ofsted, 2013, Inspecting online safety – guidance document)

Online safety – Across the curriculum

It is vital that children are taught how to stay safe, protect themselves from harm and take a responsible approach to their own and other's online safety. The school provides relevant, flexible and engaging online safety education to all children as part of their curriculum entitlement and consider the following points.

- We provide regular, planned online safety teaching within a range of curriculum areas (using the Lancashire ICT progression document) and through this document we are able to ensure online safety is progressive throughout the school.
- Children with special needs are entitled to the same online safety teaching but at an appropriate level to their needs and understanding.
- We have an additional focus on online safety during the National online safety Awareness Week.
- Through Lancashire plans we ensure children are made aware of the relevant legislation when using the internet e.g. Data Protection Act (2018) and copyright implications.
- Children are made aware of the impact of cyberbullying and how to seek help if they are affected by these issues, e.g. using peer mentoring (Anti-bullying Ambassadors) or worry boxes.
- Children are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.
- We ensure that children 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.
- Children are reminded of safe Internet use e. g. classroom displays, online safety rules (see Appendices), acceptance of site policies when logging onto the school network.

Online safety – Raising staff awareness

- A staff training needs audit has been carried out to ascertain the level of knowledge and expertise in the use of new technologies and their potential benefits and risks.
- There is a planned programme of formal online safety training and non-teaching staff to ensure they are regularly updated on their responsibilities as outlined in the school policy.
- The online safety Champion will provide advice/ guidance or training to individuals as and when required due to them receiving online safety training/ updates from external or accredited providers.
- Online safety training is provided within an induction programme for all new staff to ensure that they fully understand both the school's online safety Policy and Acceptable Use Policy.
- Regular updates on online safety Policy, Acceptable Use Policy, curriculum resources and general online safety issues are discussed in staff meetings.

Online safety – Raising parents/ carers awareness

"Parents often either underestimate or do not realize 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." (Byron Report, 2008)

St Michael and St John's school offers regular opportunities for parents/ carers and the wider community to be informed about online safety, including the benefits and risks of using various technologies both at home and at school, this is done, for example through:

- School, newsletters, homework diaries, Website and other publications.
- Bespoke Parents online safety Awareness sessions or workshops (held regularly on various days and times).
- Promotion of external online safety resources/ online materials via the school website and leaflets sent to parents.

Online safety – Raising Governors' awareness

Governors, particularly those with specific responsibilities for online safety, ICT or child protection, are kept up to date through subject reports and discussion at Governor Meetings and internal staff/ parent meetings.
The policy is regularly reviewed and approved by the governing body.

12. Evaluating the impact of the online safety Policy

It is important that schools monitor and evaluate the impact of safeguarding procedures throughout schools. We know that the online safety Policy is having the desired effect due to children/ staff and users reporting no incidents on the incident log. The online safety Champion is responsible for monitoring, recording and reviewing incidents. Incidents are analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children. These patterns are then addressed in the most effective way e.g. working with a specific groups, class assemblies or reminders for parents. Monitoring and reporting of online safety incidents contribute to changes in policy and practice through adaptation of the needs/ uses of the technology. Staff, parents/ carers, children and governors are then informed of these changes through letters, parent mail, meetings and training.

Appendices

St Michael & St John's RC Primary School
Lowergate,
Clitheroe,
Lancashire
BB7 1AG
Headteacher: Mrs Zoe Mabbott BEd (Hons) NPQH

Telephone: 01200 422560
Fax: 01200 422531
E-mail: head@ssmj.lancs.sch.uk

Appendix 1- Parents letter for taking photographs

Date

Dear Parent / Carer

We regularly take photographs/videos of children at our school and believe that these can provide a valuable record of children's learning. These may be used in children's learning journeys and profiles, our school prospectus, in other printed publications, on our school website, or in school displays.

We also actively encourage children to use school cameras to take photographs / videos as part of their learning activity.

Occasionally, our school may be visited by the media or third party who will take photographs/videos of an event or to celebrate a particular achievement. These may then appear in local or national newspapers, websites or on televised news programmes.

We recognise that increased use of technology and opportunities for online publishing mean that there is greater potential for accidental or deliberate misuse. We endeavour to minimise risks by putting safeguards in place that will protect your child's interests, and enable us to comply with the Data Protection Act (1998).

Please read and complete the attached consent form (for each child) and return to school as soon as possible. We appreciate that some families may have additional concerns and anxieties regarding protection of a child's identity and therefore request that you inform us, in writing, of any special circumstances either now or at any time in the future that may affect your position regarding consent.

Yours sincerely

Z. Mabbott

Mrs Z. Mabbott
Headteacher

APPENDIX 2

Image Consent Form

Name of the child's parent/carer:……

Name of child:……

Year group:.....

Please read the Conditions of Use on the back of this form then answer questions 1-4 below. The completed form (<u>one for each child</u>) should be returned to school as soon as possible. (Please Circle your response)

1. Do you agree to photographs / videos of your child being taken by authorised staff within the school? Yes / No

2. Do you agree to photographs / videos of your child being taken in group situations by 3rd parties at special events e.g. School productions or extra- curricular events or in the EYFS setting?

   Yes / No

3. May we use your child's image in printed school publications and for digital display purposes within school? Yes / No

4. May we use your child's image on our school's online publications e.g. website?

   Yes / No

5. May we record your child on video? Yes / No

6. May we allow your child to appear in the media as part of school's involvement in an event?

   Yes / No

In signing this form you are also agreeing not to place images/ videos of children (other than your own) on social media sites such as Facebook and Twitter without specific permission from the parents of all the included children?

I have read and understand the conditions of use attached to this form

Parent/Carer's signature: ……

Name (PRINT): ……

Date: ……..

Conditions of Use

1. This form is valid for this academic year *2018-2019.*
2. The school will not re-use any photographs or videos after your child leaves this school without further consent being sought.
3. The school will not use the personal contact details or full names (which means first name **and** surname) of any pupil or adult in a photographic image, or video, on our website or in any of our printed publications.
4. If we use photographs of individual children, we will not use the full name of that pupil in any accompanying text or caption.
5. If we use the full name of a pupil in the text, we will not use a photograph of that pupil to accompany the article.
6. We will only use images of children who are suitably dressed and in a context that is not open to misinterpretation.
7. 3rd Parties may include other children's parents or relatives e.g. attending a school production.
8. Images / videos will be stored according to Data Protection legislation and only used by authorised personnel.
9. Parents should note that websites can be viewed throughout the world and not just in the United Kingdom, where UK law applies.

Notes on Use of Images by the Media

If you give permission for your child's image to be used by the media then you should be aware that:

1. The media will want to use any images/video that they take alongside the relevant story.
2. It is likely that they will wish to publish the child's full name, age and the school's name in the caption for the picture (possible exceptions to this are large group or team photographs).
3. It is possible that the newspaper will re-publish the story on their website or distribute it more widely to other newspapers or media organisations.

<u>Appendix 3</u> - Consent Form for Images to be Taken e.g. at a School Production or Special Event

Dear Parent/ Carer,

Your child will be appearing in annual school productions such as Christmas and Easter concerts. We are aware that these events are special for children and their relatives / friends and form treasured memories of their time at school.

We have a rigorous policy in place with regard to taking, using and publishing images of children and you have already signed a consent form stating whether you agree to your child's images / video being used in general circumstances.

Many parents / carers like to take photographs / videos of their children appearing in school productions, but there is a strong possibility that other children may be included in the pictures. In these circumstances, we request specific consent for images / videos to be taken by a third party (i.e. other parents). We need to have permission from all parents / carers of children involved in the production to ensure that they are happy for group images / videos to be taken and I would be grateful if you could complete the slip at the bottom of this letter and return to school as soon as possible.

We would also request that images / videos including other children or adults are not posted online, especially on Social Media sites e.g. Facebook without the specific permission of the individuals included in the footage.

Should any parents / carers not consent, we will consider other options, e.g. arranging specific photo opportunities after the production.

These decisions are not taken lightly, but we have to consider the safeguarding of all our children and respect parents' rights to privacy.

Yours sincerely,

Mrs Mabbott
(Headteacher)

Child's name: _____ Date: _____

I agree/ do not agree to photographs/ videos being taken by third parties at the annual productions.

Signed: _____ (parent/ carer)

Print name: _____

APPENDIX 4

ICT Acceptable Use Policy (AUP) – Staff and Governors

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs Mabbott.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in online safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with children and other adults are appropriate.
8. I will not use the school system(s) for personal use during working hours.
9. I will not install any hardware or software without the prior permission of Mrs Mabbott.
10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
12. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
13. I will report any known misuses of technology, including the unacceptable behaviours of others.
14. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
15. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
16. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
17. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
18. I am aware that in certain circumstances where unacceptable use is suspected, enhanced

monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.

19. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's online safety policy and help children to be safe and responsible in their use of ICT and related technologies.
20. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……..

Date ……..

Full Name …….…… (PRINT)

Position/Role ……

APPENDIX 5

ICT Acceptable Use Policy (AUP) – Students, Supply Teachers, Visitors, Guests etc.

To be signed by any adult working in the school for a short period of time.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
3. I will not use any external device to access the school's network e.g. pen drive.
4. I will respect copyright and intellectual property rights.
5. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
6. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
7. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
8. I will not install any hardware or software onto any school system.
9. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……..

Date ……..

Full Name …… (PRINT)

Position/Role ……

Appendix 6

ICT Acceptable Use Policy (AUP) - Children

These rules reflect the content of our school's online safety Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

- ✓ I will only use ICT in school for school purposes.
- ✓ I will not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher.
- ✓ I will only use the Internet and/or online tools when a trusted adult is present.
- ✓ I will only use my class e-mail address or my own school email address when emailing.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- ✓ I will not deliberately bring in inappropriate electronic materials from home.
- ✓ I will not deliberately look for, or access inappropriate websites.
- ✓ If I accidentally find anything inappropriate I will tell my teacher immediately.
- ✓ I will only communicate online with people a trusted adult has approved.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not give out my own, or others', details such as names, phone numbers or home addresses.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will not arrange to meet anyone that I have met online.
- ✓ I will only open/delete my own files.
- ✓ I will not attempt to download or install anything on to the school network without permission.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my online safety.
- ✓ I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy.

……**Parent/ Carer Signature**

We have discussed this Acceptable Use Policy and
…….... [Print child's name] agrees to follow the online safety rules and to support the safe use of ICT at St Michael and St John's School.

Parent /Carer Name (Print) ……

Parent /Carer (Signature) ……. ……

Class …… Date.....

This AUP must be signed and returned before any access to school systems is allowed.

St Michael & St John's RC Primary School
Lowergate,
Clitheroe,
Lancashire
BB7 1AG
Headteacher: Mrs Zoe Mabbott BEd (Hons) NPQH

Telephone: 01200 422560
Fax: 01200 422531
E-mail: head@ssmj.lancs.sch.uk

Appendix 7 ICT Acceptable Use Policy (AUP) Parent's letter <Date>

Dear Parent/Carer,

The use of ICT including the Internet, e-mail, learning platforms and mobile technologies are integral elements of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all children to act safely and responsibly when using technology both within, and outside of, the school environment.

In school, we ensure that all resources used by the children are age appropriate and suggest that parents check the terms and conditions for the use of online resources and games to ensure that resources used at home are also age appropriate. This is particularly relevant when using Social Network Sites that incorporate age-restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of the site's privacy policy and / or terms and conditions and therefore we actively discourage this in our school.

The enclosed ICT Acceptable Use Policy forms part of the wider School online safety Policy and alongside the school's Behaviour and Safeguarding Policies outlines those principles we expect our children to uphold for the benefit of both themselves and the wider school community.

Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible. Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguard the children in school.

Along with addressing online safety as part of your child's learning, we will also be holding Parental online safety Awareness Sessions during the school year and I would take this opportunity to strongly encourage your attendance wherever possible. Further information on these sessions will be communicated as soon as dates are confirmed. In the meantime, if you would like to find out more about online safety for parents and carers, please visit the Lancsngfl online safety website http://www.lancsngfl.ac.uk/online safety

If you have any concerns or would like to discuss any aspect of the use of ICT in school, please contact Mrs Jackson.
Yours sincerely,

Z. Mabbott

Mrs Z. Mabbott
Headteacher

Appendix 8
Classroom online safety Rules (EYFS/ KS1)

Our Golden Rules for Staying Safe with ICT

We only use the Internet when a trusted adult is with us.

We are always polite and friendly when using online tools.

We always make careful choices when we use the Internet.

We always ask a trusted adult if we need help using the Internet.

We always tell a trusted adult if we find something that upsets us.

Appendix 9
Classroom online safety Rules (KS2)

Our Golden Rules for Staying Safe with ICT

We always ask permission before using the Internet.

We only use the Internet when a trusted adult is around.

We immediately close/ minimise any page we are uncomfortable with (or if possible switch off the monitor).

We always tell an adult if we see anything we are uncomfortable with.

We only communicate online with people a trusted adult has approved.

All our online communications are polite and friendly.

We never give out our own, or other's personal information or passwords and are very careful with the information that we share online.

We only use programmes and content which have been installed by the school.

St Michael & St John's RC Primary School
Lowergate,
Clitheroe,
Lancashire
BB7 1AG
Headteacher: Mrs Zoe Mabbott BEd (Hons) NPQH

Telephone: 01200 422560
Fax: 01200 422531
E-mail: head@ssmj.lancs.sch.uk

Appendix 10 – Letter to parents regarding Parental online safety Awareness Session

<date>

Dear Parent/Carer,

Having access to online information and the opportunities that the digital world can offer has many benefits and for some it plays an important part of our everyday lives. However, as technology moves on at such a pace, it is sometimes difficult to keep up with new trends and developments, particularly with regard to mobile/games technologies and secure and safe accessibility to online material.

Our school has policies in place to ensure our children are learning in a safe and secure environment which includes being safe online. This session has been organised to help you to contribute to the process of helping your child to be aware of the potential risks associated with using the Internet and modern technologies.

Ofsted increasingly view Parental online safety Awareness sessions as essential components of effective safeguarding provision and I would therefore appreciate your support in attending this event.

We will be hosting the above session on the Date/Time below and I would strongly encourage your attendance:

Date:……Time:……

The session will include reference to the following areas with time for you to ask questions:

- ✓ What are our children doing online and are they safe?
- ✓ Do they know what to do if they come across something suspicious?
- ✓ Are they accessing age-appropriate content?
- ✓ How can I help my child stay safe online?

Yours sincerely,
Z. Mabbott

Mrs Z. Mabbott
Headteacher

I / we will be attending the above Parental online safety Awareness Session Name(s):……

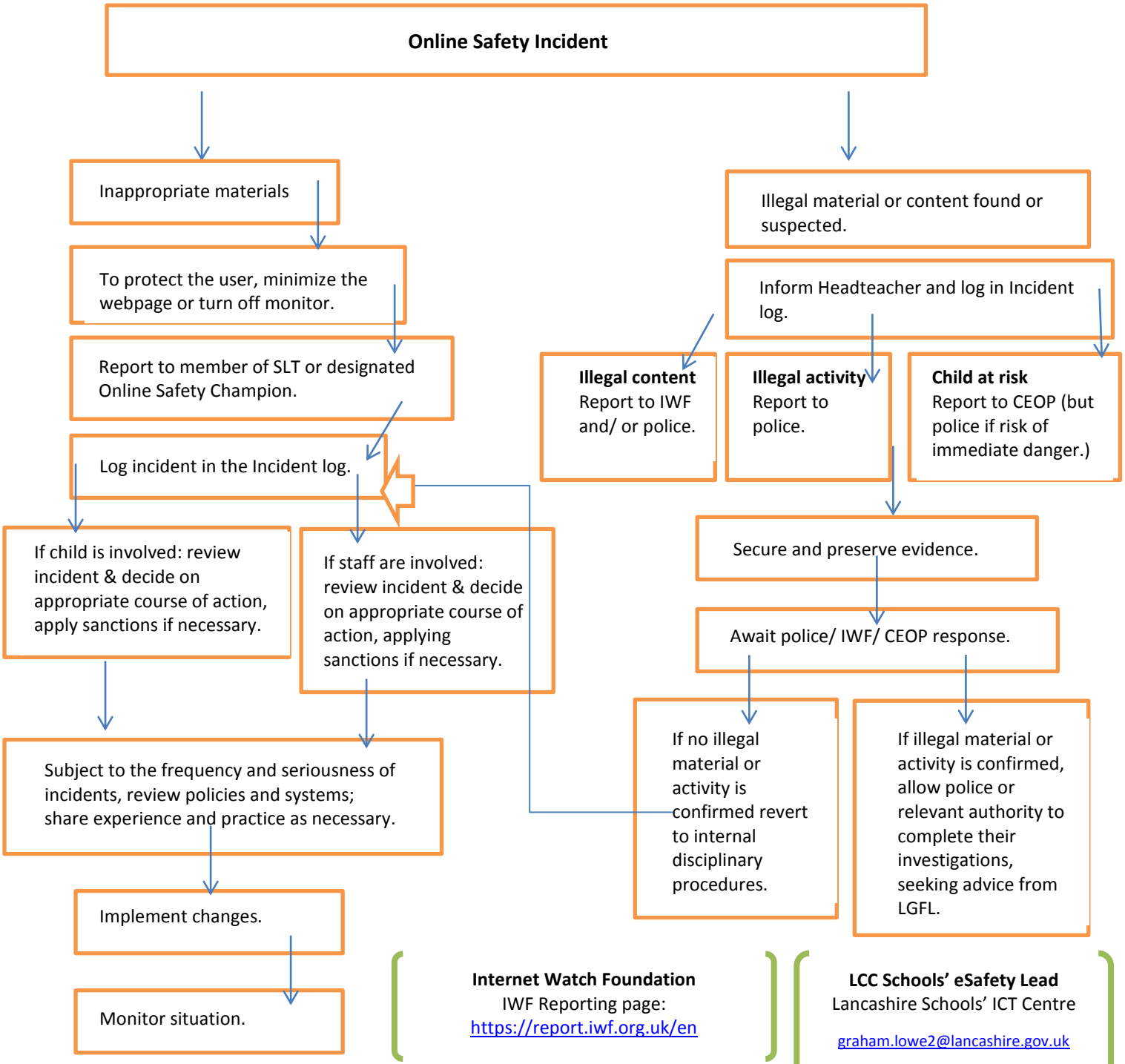
Parent / Carer of:……Year Group……

Appendix 11
online safety Incident Log

All online safety incidents must be recorded by the School online safety Champion or designated person. This incident log will be monitored and reviewed regularly by the Headteacher and Chair of Governors.

Date / time of incident	Type of Incident	Name of pupils/ and staff involved	System details	Incident details	Resulting actions taken and by whom (and signed)
01 Jan 2010 9.50 am	Accessing Inappropriate Website	A N Other (Pupil) A N Staff (Class Teacher)	Class 1 Computer 1.5	Pupil observed by Class Teacher deliberately attempting to access adult websites.	Pupil referred to Headteacher and given warning in line with sanctions policy for 1st time infringement of AUP. Site reported to LGFL as inappropriate.

Appendix 12
Responding to online safety Incident / Escalation Procedures



Internet Watch Foundation
IWF Reporting page:
https://report.iwf.org.uk/en

LCC Schools' eSafety Lead
Lancashire Schools' ICT Centre
graham.lowe2@lancashire.gov.uk

Lancashire Constabulary
Neighbourhood Policing Team
www.lancashire.police.uk/contact-us
0845 1 25 35 45

Chile Exploitation and Online Protection Centre (CEOP)
CEOP Reporting page:
www.ceop.gov.uk/reportabuse/index.asp

Securing and Preserving Evidence- Guidance notes

The system used to access the suspected illegal materials or activity should be secured as follows:

- Turn off the monitor (Do NOT turn off the system)
- Ensure the system is NOT used or accessed by any other persons (including technical staff)
- Make a note of the date/ time of the incident along with relevant summary details.

Contact your School's Neighbourhood Policing Team for further advice.