Fremington Community Primary & Nursery School

eSAFETY POLICY

Policy Information

Statutory/Non-Statutory:	Statutory
Approved/Reviewed by:	Teaching & Learning Committee
Model:	School
Version:	January 2017
Last reviewed/approved:	January 2018
Minute Ref:	T&L Jan 2018/13.3
Review Due:	January 2019 (annual)

Contents

This document will be used in conjunction with Fremington CP's Behaviour Policy.

1. Introduction

Our eSafety Policy should be read in conjunction with other related school policies and documents.

Policies and documents to consider	How is eSafety included?
School Self Evaluation Framework	E-safety features are part of the safeguarding elements of the school
School Improvement Plan E-safety	E-safety has been highlighted in the ICT area of the school development plan
Staff Code of Conduct, Recruitment and Induction Procedures	All staff have signed an Acceptable Use Policy regarding the use of ICT in school
Anti Bullying Policy	Cyberbullying is part of the anti-bullying policy
Behaviour Policy	The acceptable use of technology is included in our Behaviour Policy. There are clear guidelines for dealing with eSafety issues.
Child Protection Policy	The Child Protection Policy includes references to digital media

2. Fremington CP school's vision for eSafety

Fremington provides a diverse, balanced and relevant approach to the use of technology.

- Through a variety of media the children are encouraged to maximise the benefits and opportunities that technology has to offer.
- The school aims to ensure that children learn in an environment where security measures are balanced appropriately with the need to learn effectively
- The children are increasingly being equipped with the skills and knowledge to use technology appropriately and responsibly.
- The school aims to recognise the risks associated with technology and how to deal with them, both within and outside the school environment
- The users in the school community understand why there is a need for an eSafety Policy.

3. The role of the Senior Management Team.

The role of the Senior Management Team and eSafety co-ordinator include:

- Having operational responsibility for ensuring the development, maintenance and review of the school's eSafety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an eSafety incident occur.
- Ensuring the eSafety Incident Log is appropriately maintained and reviewed termly.
- Keeping personally up-to-date with eSafety issues and guidance through liaison with the Local Authority Schools' ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging eSafety advice/training for staff, parents/carers and governors.
- Ensuring the Headteacher, SMT, staff, pupils and Governors are updated as necessary.

- Liaising closely with the school's Designated Senior Person / Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.

4. Policies and Practices

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

4.1 Security and data management

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 must be:

- 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 laptops are password protected

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

- The Senior Leadership Team are responsible for managing information
- Staff are aware of where data is located
- All staff with access to personal data understand their responsibilities.
- The school ensures that data is appropriately managed both within and outside the school environment .
- The staff are aware that they should only use approved means to access, store and dispose of confidential data
- Staff have access to school logins, to ensure the data remains secure.
- The school aims to ensure that data loss is managed by the use of passwords for the required people
- The school's procedure for backing up data is on discs which are replaced on a regular basis.

4.2 Use of mobile devices

The use of mobile devices offers a range of opportunities to extend children's learning. Staff are aware that some mobile devices e.g. mobile phones, game consoles or net books can access unfiltered internet content.

- Mobile phones are not encouraged to be brought into school by children . If a phone is brought in by mistake or is needed after school the children are asked to hand the phone in to a teacher or taken to the office.

4.3 Use of digital media

Various forms of digital media offer substantial benefits to education but equally present schools with challenges particularly regarding posting or sharing media on the Internet, through mobile technologies and Social Network sites. To ensure all users are informed and educated about the risks surrounding taking, using, sharing, publishing and distributing digital media, any images taken at school will only be used for school purposes e.g. website, brochure or display.

- All school photographs and video of pupils and staff are regarded as personal data in terms of The Data Protection Act (1998), and the school has written permission for their use from the individual and/or their parents or carers.
- The school seeks consent from the pupil, parent/carer or member of staff who appears in the media or whose name is used
- The parental/carer permission is obtained on entry to the nursery/school but the parents have a right to change this if deemed necessary.
- The staff and pupils aware that full names and personal details will not be used on any digital media, particularly in association with photographs.
- Parents/carers, who have been invited to attend school events are allowed to take videos and photographs **on the understanding that they do not publish them or share them on the internet.**
- All staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites.
- The school ensures that photographs/videos are only taken using school equipment and only for school purposes.
- The school ensures that any photographs/videos are only accessible to the appropriate staff/pupils.
- Staff are encouraged not to store digital content on personal equipment. The staff are encouraged **not to use their own cameras or other digital capturing devices**
- When taking photographs/video, staff ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted.
- Staff, parents/carers and pupils made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved.
- The guidelines for safe practice relating to the use of digital media, as outlined in the school's policy are monitored by the S.M.T and Governors on an annual basis.

4.4 Communication technologies

School uses a variety of communication technologies and is aware of the benefits and associated risks.

Email

- All users have access to the South West Grid for Learning gmail service- this is a filtered system
- Only official email addresses are used between staff and with pupils/parents when personal/sensitive data is involved.
- The South West Grid for Learning filtering service reduces the amount of SPAM (Junk Mail) received on school email accounts.

- All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- All school-based communications may be monitored at any time in accordance with the Acceptable Use Policy.
- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- Our school includes a standard disclaimer at the bottom of all outgoing emails (see below).

Fremington CP & Nursery School's email disclaimer

……

Emails and any attachments from Fremington Community Primary & Nursery School are confidential.
If you are not the intended recipient, please notify the sender immediately by replying to email, and then delete it without making copies or using it in any way.
Although any attachments to the message will have been checked for viruses before transmission, you are urged to carry out your own virus check before opening attachments, since Devon County Council accepts no responsibility for loss or damage caused by software viruses.
Senders and recipients of email should be aware that under the UK Data Protection and Freedom of Information legislation these contents may have to be disclosed in response to a request.

Social Networks

Social Network sites allow users to be part of a virtual community. Current popular examples of these are Facebook, Twitter and Club Penguin. These sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a blog or comments published by the user. As a user on a Social Network site, you may have access to view other users' content, send messages and leave comments.

All staff need to be aware of the following points:

- They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
- Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- If a Social Network site is used, details must not be shared with pupils and privacy settings be set at maximum.
- Pupils **must not, and** parents **should not** be added as 'friends' on any Social Network site.
- Children who are under 13 are not legally allowed to be members of Facebook.

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

Mobile telephone

- The school allows personal mobile phones to be used in school by staff and visitors but are asked to be left on silent in curriculum time and to be used only in the staffroom or outside school gates.

- It is acceptable to use personal mobile phones for school activities e.g. school trips.

Web sites and other online publications

This may include for example, podcasts, videos, 'Making the News' and blogs.

- The school website is effective in communicating eSafety messages to parents/carers.
- Everybody in the school is made aware of the guidance for the use of digital media on the website.

- Everybody in the school aware of the guidance regarding personal information on the website.

- The Head teacher and governing body has overall responsibility for what appears on the website.

Others

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

4.5 Acceptable Use Policy (AUP)

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

AUPs are used for Staff and pupils and must be signed and adhered to by users before access to technology is allowed. This agreement is as a partnership between parents/carers, pupils 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.

Our school AUPS aim to:

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

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

4.6 Dealing with incidents

At Fremington CP an incident log (see appendix) is completed to record and monitor offences. This is audited on a regular basis by the eSafety co-ordinator or other designated member of the Senior Management Team.

Illegal Offences

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). **Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence.** It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Any potential illegal content would be reported to the Internet Watch Foundation (http://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 content
- Incitement to racial hatred

More details regarding these categories can be found on the IWF website http://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 proportionate to the offence. The school will decide what constitutes inappropriate use and the sanctions to be applied.

Some examples of inappropriate incidents are listed below with suggested sanctions.

Incident	Procedure & Sanctions
Accidental access to inappropriate materials.	• Minimise the webpage/ Turn the monitor Off • Tell a trusted adult. • Enter the details in the Incident Log and report to the SMT and ICT Technician if necessary. • Persistent 'accidental' offenders may need further disciplinary action.
Using other people's logins and passwords maliciously.	• Inform SMT or designated eSafety coordinator. • Enter the details in the Incident Log. • Additional awareness raising of eSafety issues and the AUP with individual
Deliberate searching for inappropriate materials.	• Inform SMT or designated eSafety coordinator.

	• Enter the details in the Incident Log. • Additional awareness raising of eSafety 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.
Bringing inappropriate electronic files from home.	• As above
Using chats and forums in an inappropriate way.	• As above

- The Leadership team is responsible for dealing with eSafety incidents. All staff are aware of the different types of eSafety incident and how to respond appropriately. e.g. illegal or inappropriate.
- Procedures are in place to deal with eSafety incidents and all staff aware of these.
- Children are informed of the procedures through discussions with members of staff.
- These incidents are logged in a log book kept in the office
- Incidents are monitored, by the SLT on a regular basis.
- The measures that are in place to respond to and prevent recurrence of an incident.
- The SMT will decide at which point parents or external agencies are involved.
- The procedures are in place to protect staff and escalate a suspected incident/allegation involving a staff member (See Appendix)

The school uses the 'eSafety Incident/ Escalation Procedures' document (See Appendix) as a framework for responding to incidents.

5. Infrastructure and Technology

The school ensures that the infrastructure/network is as safe and secure as possible. Broadband connection, filtering and virus protection are provided (by default) by the South West Grid for Learning.

Pupil access

- The children are supervised by staff when accessing school equipment and online materials

Passwords

- All users of the school network have a secure username and password.
- The administrator password for the school network available to the Headteacher and other nominated senior leader is kept in the school office.
- Staff and pupils are reminded of the importance of keeping passwords secure
- Passwords will be changed regularly

Software/hardware

The school has legal ownership of all software.

- The school has an up to date record of appropriate
- The school has an up to date record of appropriate licences for all software and the ICT technician is responsible for maintaining this.

Managing the network and technical support

- Servers, wireless systems and cabling are securely located and physical access restricted.
- The SLT is responsible for managing the security of the school network.
- The safety and security of the school network Is monitored on a regular basis.
- The school systems are kept up to date in terms of security e.g computers are regularly updated with critical software updates/patches.
- Users (staff, pupils, guests) have clearly defined access rights to the school network e.g. they have a username and password.
- Staff and pupils are encouraged to lock or log out of a school system when a computer/digital device is left unattended.
- Only the administrator and ICT Technician are allowed to download executable files and install software.
- Users report any suspicion or evidence of a breach of security to the Leadership team
- The school encourages teachers to follow esafety policy guidelines when using laptop for personal/family use
- If network monitoring takes place, it is in accordance with the Data Protection Act (1998)
- The SLT is responsible for liaising with/managing the technical support staff.

6. Education and Training

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

The main areas of eSafety risk that we need to consider:

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

6.1 eSafety across the curriculum

It is vital that pupils are taught how to take a responsible approach to their own eSafety. Fremington provides suitable eSafety education to all pupils:

- Regular, planned eSafety teaching within a range of curriculum areas using the school ICT Progression Framework.
- E-Safety education is differentiated for pupils with special educational needs.
- Pupils are made aware of the impact of Cyberbullying and how to seek help if they are affected by these issues.
- Pupils are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.
- The school ensures that pupils develop an understanding of the importance of the Acceptable Use Policy and are encouraged to adopt safe and responsible use of ICT both within and outside school.
- Pupils are reminded of safe Internet use e.g. classroom displays, eSafety rules etc.

6.2 eSafety – Raising staff awareness

- There is a programme of formal eSafety training for all staff to ensure they are regularly updated on their responsibilities as outlined in our school policy.
- The eSafety co-ordinator provides advice/guidance or training to individuals as and when required.
- The eSafety training ensures staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites.
- All staff are expected to promote and model responsible use of ICT and digital resources.
- Esafety training is provided within an induction programme for all new staff to ensure that they fully understand both the school's eSafety Policy and Acceptable Use Policy.
- Regular updates on eSafety Policy, Acceptable Use Policy, curriculum resources and general eSafety issues are discussed in staff/team meetings.

6.3 eSafety – Raising parents/carers awareness

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

The school offers opportunities for parents/carers and the wider community to be informed about eSafety, including the benefits and risks of using various technologies. For example through:

- School newsletters, Website, and other publications.
- Promotion of external eSafety resources/online materials.

6.4 eSafety – Raising Governors' awareness

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

NB The eSafety Policy will be reviewed yearly (and/or if a serious breach occurs earlier) by the eSafety coordinator and SMT, approved by the governing body and made available on request.

List of Appendices

Appendix 1

Fremington CP & Nursery School's – Image Consent Form

Name of the child's parent/carer: _____

Name of child:_____

Year group:_____

We regularly take photographs/videos of children at our school. These may be used in our school prospectus, in other printed publications, on our school website, or in school displays.

Occasionally, our school may be visited by the media 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.

In order that we can protect your child's interests, and to comply with the Data Protection Act (1998), **please read the Conditions of Use on the back of this form, then answer questions 1-4 below. Please sign, date and return the completed form (one for each child) to school as soon as possible.**

(Please Circle)

1. May we use your child's photograph in printed school publications and for display purposes? .....Yes / No

2. May we use your child's image on our school website? ..... Yes / No

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

4. May we allow your child to appear in the media as part of school's involvement in an event? ..... Yes / No

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 the length of time that your child is at Fremington C P & Nursery School.
2. 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
3. If we use photographs of individual pupils, we will not use the full name of that pupil in any accompanying text or caption.
4. 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.
5. We will only use images of pupils who are suitably dressed.
6. 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 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.

Appendix 2

Fremington CP & Nursery School's - ICT Acceptable Use Policy Staff and Governor Agreement

ICT and the related technologies such as email, 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 the Headteacher.

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 eSafety 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, pupils 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 pupils and other adults are appropriate.
8. I will not use the school system(s) for personal use in working hours (except for use during breaks/lunchtimes.)
9. I will not install any hardware or software without the prior permission of the SMT.
10. I will ensure that personal data is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will ensure that Images of pupils 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 per son/s in the image.
12. I will report any known misuses of technology, including the unacceptable behaviours of others.
13. 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.
14. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
15. 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.
16. I understand that network activities and online communications may be monitored, including any personal and private communications made using school systems.

17. 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.
18. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's eSafety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
19. 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 3

Fremington CP & Nursery School's - ICT Acceptable Use Policy Supply teachers and Visitors/Guests Agreement

For use with any adult working/helping 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 respect copyright and intellectual property rights.
4. I will ensure that Images of pupils 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.
5. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
6. I will not install any hardware or software onto any school system.
7. 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 4

Fremington CP & Nursery School's- ICT Acceptable Use Policy Pupils Agreement / eSafety Rules

These rules are a reflection of the content of our school's eSafety 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 only use the Internet and/or online tools when a trusted adult is present.
- ☺ I will only use my class email 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 eSafety.
- ☺ 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 eSafety rules and to support the safe use of ICT at Fremington CP. & Nursery School.

Parent /Carer Name (Print) ……

Parent /Carer (Signature) ……..

Class …… Date……

Appendix 5

ICT Acceptable Use Policy (AUP) – Parents' Letter

Fremington CP & Nursery School

Dear Parent/ Carer,

The use of ICT including the Internet, email, learning platforms and today's mobile technologies are an integral element of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all pupils to act safely and responsibly when using technology both within, and outside of, the school environment.

This is particularly relevant when using Social Network Sites which are becoming increasingly popular amongst both the adult population and young people. However, many sites do have 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 these age-restriction policies and therefore we actively discourage this in our school.

The enclosed ICT Acceptable Use Policy forms part of the wider School eSafety Policy and alongside the school's Behaviour Policy outlines those principles we expect our pupils 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 safeguards the pupils in school.

If you have any concerns or would like to discuss any aspect of the use of ICT in school, please contact the Hedateacher or any member of the school's Senior Management Team.

Yours sincerely,

Appendix 6

eSafety 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 7

eSafety Rules (KS2)

OurGolden 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 others', personal information or passwords and are very careful with the information that we share online.

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

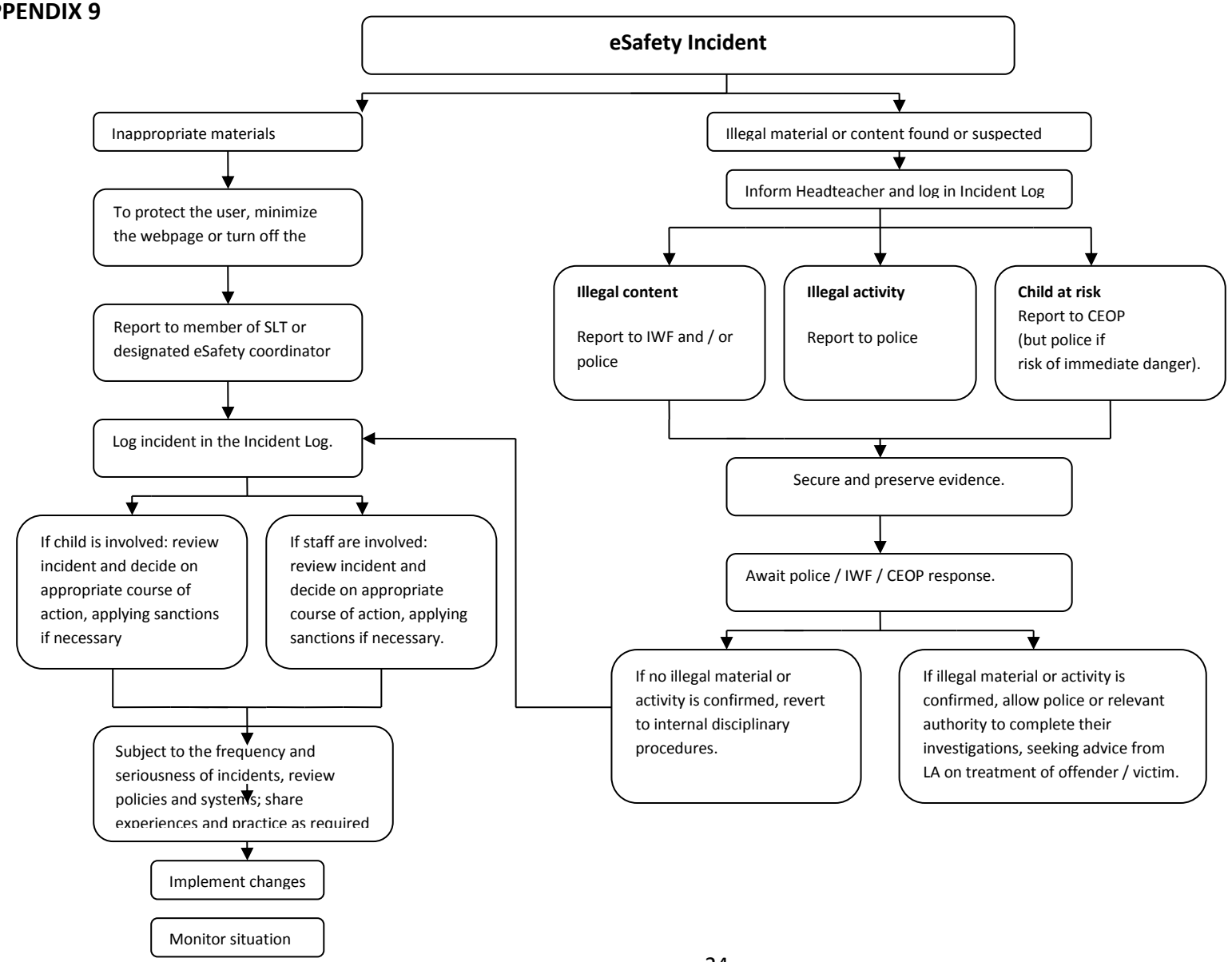
APPENDIX 8

Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

APPENDIX 9



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 (inc. 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

Policy Date	Summary	Minute Reference	Chair of Governors
22/03/2012	Policy Adopted	5.4-2011/12	S Miller
12/12/2013	Policy Reviewed	9.8-2012/13	S Miller
11/12/2014	Policy Reviewed	9.3-2014/15	S Miller
1/2/2017	Policy Reviewed		
Jan 2018	Policy Reviewed	Jan 2018/13.3	T&L