Marine Park First School E-Safety policy

Contents

1. Roles and Responsibilities

The e-Safety Policy relates to other policies including those for ICT, bullying and for child protection. Miss Scott and Mr. Easton are the e-Safety Coordinators.

Our e-Safety coordinator's responsibilities are:

- to ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as The Child Exploitation and Online Protection (CEOP);
- to ensure the senior leadership and Governors are updated as necessary;
- ensuring that the policy is implemented and that compliance with the policy is actively monitored;
- ensuring all staff are aware of reporting procedures and requirements should an eSafety incident occur;
- ensuring the eSafety Incident Log is appropriately maintained and regularly reviewed;
- providing or arranging eSafety advice/training for staff, parents/carers and governors;
- liaising closely with the school's Designated Senior Person / Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas including the Prevent Duty.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a culture where pupils feel able to report any bullying, abuse or inappropriate materials(reference: Safe to Learn policy).

All staff should be familiar with the schools' policy including:

- Safe use of Internet including use of internet-based communication services, such as instant messaging and social networks;
- Safe use of school network, equipment and data storage;
- Safe use of digital images and digital technologies, such as mobile phones, tablets, digital cameras;
- Publication of pupil information/photographs and use of website;
- EBullying / Cyberbullying procedures;
- Their role in providing e-Safety education for pupils;

Appendix three outlines detailed guidance to staff and the code of conduct relating to ICT.

Staff are reminded / updated about e-Safety matters annually.

Our e-Safety Policy has been written by the school, building on the Kent e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.

The e-Safety Policy was revised by: 25.1.16

It was approved by the Governors on: Summer 2016

In January 2016 the LA ICT consultant supported us to review and update or E-Safety Policy and practice.

2. Teaching and learning

Why the Internet and digital communications are important

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

The Technologies

New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- the internet;
- e-mail;
- Videochat;
- Instant messaging, often using simple web cams;
- Blogs (an on-line interactive diary);
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player);
- Social networking sites;
- Video broadcasting sites;
- Chat Rooms;
- Gaming Sites;
- Music download sites;
- Mobile phones with camera and video functionality;
- Smart phones;
- Tablets;
- eReaders;

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and effective curriculum practice;
- communication and collaboration with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the LA and DFE;
- access to learning wherever and whenever convenient.

Internet use will enhance learning

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
Pupils will be taught the importance of cross-checking information before accepting its accuracy.
Pupils will be taught how to report unpleasant Internet content e.g. locally, to school staff, and online using report mechanisms such as the CEOP '*Report Abuse*' icon or Hector Protector.

3. Security and data management

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security

- *Pupil data and photographs must only be stored on the school network or school equipment (ipads/cameras). Pupil data must only be stored on the staff drive.*
- *Staff may use external USB drives but can only store sensitive information such as pupil data on encrypted memory drives provided by the school.*
- *Sensitive information such as pupil data must not be stored in Cloud storage.such as Google Drive*
- *Laptops are securely locked away at the end of the day if being left on the premises or if being taken home, are never left unattended in vehicles etc.*

Passwords

In our school, all ICT password policies are the responsibility of the Headteacher and e-safety coordinator and all staff and pupils are expected to comply with the policies at all times

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security. Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others. Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the school network is 6.30pm

Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) log-in username. From Year 3 they are also expected to use a personal password for the Learning Platform and keep it private. All users of the school network have a secure username and password and should only use personal passwords to access computer based services.

All staff and pupils are reminded of the importance of keeping passwords secure, they are informed not to write these passwords down at any time. If a pupil or member of staff believe that someone other than themselves has become aware of their password, they are to report to the eSafety coordinator or ICT Co-cordinator and their password will be changed.

Staff will be prompted to change NTLP and SIMS passwords in line with NT password policy.

Staff iPads must have a pass-code installed to the lock-screen of the device. Users must not share this pass-code with others.

Password Security
Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer)

Starters and Leavers

Adults who work in schools may have access to a range of important and sensitive information including images and personal details of colleagues and learners and it is essential that the integrity of the school's systems and files remain intact when colleagues leave the school.

To help ensure that a school's data and resources remain secure as personnel leave the organisation User ID/email and passwords for staff and pupils who have left the School will be removed from the system/disabled within 4 weeks.

Filtering and virus protection:
Annual virus protection is purchased for the network and all school computers. Regular scans should be performed by staff on devices that are not connected to the Network.

Any device suspected or found to contain any virus or malware must be immediately turned off and removed from the network. The ICT coordinator must then be informed so appropriate technical support can be sought.

Internet filtering is provided by the Local Authority as part of the ICT SLA. The SLA states that as part of this the LA " Provide robust filtering and security management which has been upgraded to ensure it is flexible and exceeds national expectations." While strong filters are in place, no filtering is 100% effective and so staff must remain vigilant for inappropriate content when using the internet. If anything inappropriate is found staff should turn off the screen of the machine and remove it from use. They should then (if possible) screen capture the website and report it to the e-Safety Coordinators and also ict.helpdesk@northtyneside.gov.uk so it can be reviewed and blocked if necessary.

Staff may also request for websites to be unblocked if they believe they are appropriate for educational purposes by contacting the LA corporate ICT helpdesk at ict.helpdesk@northtyneside.gov.uk

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

School ICT systems security will be reviewed regularly and security strategies will be discussed with the Local Authority.

Any material that the school believes is illegal must be reported to appropriate agencies such as the Internet Watch Foundation (IWF) or CEOP: Child Exploitation and Online Protection Centre

4. Infrastructure and technology

Pupil Access
Pupils are informed of available, appropriate materials to use and are supervised by a member of staff when accessing school equipment and online materials, at all times.

Software/hardware
All software has been purchased by the school and is the legal owner. The dates of appropriate licenses are

recorded and kept with the secure passwords in the school office. The LA technician loads any new software onto the schools network.

School laptops and iPads are for school use only.

Managing the network and technical support

The server and cabling is securely located and its physical access is restricted. The network is managed by the LA via an annual SLA. All staff should log off or lock a computer when they leave a computer / digital device unattended. A central request file is updated for LA technical support. The network is monitored via the council.
Requests for technical support can be made to support@ntlp.org.uk

5. Communication Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

The senior leadership team should note that technologies such as mobile phones with cellular Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Mobile Devices

In our school we recognise the use of mobile devices offers a range of opportunities to extend children's learning. At this point in time we do not allow children to bring in or use their own mobile devices in school.

Some staff have a laptop and class sets of laptops are available to all year groups in school for curriculum use. Acceptable use of the devices are covered in staff and student Acceptable Use Policy (AUP) documents.

Mobile device management.

All iPads in school are managed with a Mobile Device Management (MDM) system. We currently use the Meraki MDM solution for this. This allows monitoring and remote management of many features of the device, plus the ability to impose restrictions on the device, such as removing the ability to delete apps or use the camera. Apps are only added to pupil devices via the MDM system. Pupils do not have the ability to add new apps. The school business manager, ICT coordinator and the headteacher keep ownership of the school Apple ID password and must approve all new app installs on pupil devices.

The school has registered with the Apple Volume Purchase Program (VPP) and all apps are bought via this system. Licences for apps bought are recorded within the VPP account.

Mobile telephones

Our school allows personal mobile phones to be used in school by staff and visitors, however they are not to be used within the classroom or when pupils are present. Phones should be turned off or on silent during lessons.

Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by any means is forbidden.

Mobile phone technology must not be used to take photographs anywhere within the school grounds, unless

consent has been explicitly granted by the Headteacher.

Staff should only contact a parent/carer on a school telephone.

When children undertake a school trip or journey, personal mobile phone use by adult leaders should be limited to contact with the school office or venues being visited, except in emergencies.

It is not acceptable to use personal mobile phones to support lessons.

Electronic Mail

The government encourages the use of e-mail as an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects. However, un-regulated e-mail can provide a means of access to a pupil that bypasses the traditional school boundaries. In the school context, therefore, email is not considered private and is monitored by staff, whilst trying to achieve a balance between monitoring that is necessary to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

Staff and pupils may only use approved e-mail accounts on the school system. All users have access to the NTLP Google mail via our VLE (The North Tyneside Launch Pad) as the preferred school e-mail system.

Pupils must immediately tell a teacher if they receive offensive e-mail.

In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

The school should consider how e-mail from pupils to external bodies is presented and controlled.

Whole-class or group e-mail addresses are used at Key Stage 1 and below.
E-mail sent to an external organisation is written carefully and authorised before sending, in the same way as a letter written on school headed paper.
The sending of abusive or inappropriate email messages is forbidden.
Electronic mail should only be used in the course of work as a school employee and only using the authorised logins provided by the school/ Platform.

Users must never use electronic mail to send or forward chain letters or any material which may contravene School policies (e.g. jokes, pictures of a racist or sexist nature).

Users must only copy messages (i.e. cc or bcc) to people where it is of direct relevance.

Staff are expected to check their email mailboxes regularly.

There is the facility within NTLP mail to report any message to the NT ICT team as Spam or a publishing attempt. This can be done by selecting a message and clicking the exclamation mark (!) at the top of the page, or from within an email from the drop-down menu.

The use of personal web based email in school is forbidden for both staff and students so as to minimise the risk of unsuitable materials and viruses from external email accounts, e.g. Hotmail, Yahoo Mail etc, in school.

All users are made aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.

All users are made aware that all email 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.

"Sent from North Tyneside's Learning Platform
(www.ntlp.org.uk), an educational virtual learning environment.
This email may not reflect the views of the organisation.
If this email causes any concern please contact report@ntlp.org.uk."

Staff are required to add a standardised email signature covering Name, Role in school and contact details.

To do so staff can click on the cog in the top right, then 'settings', then scroll down to signature' where the passage can be pasted in and details added.

Social Networking and Personal Publishing:

Social Network sites allow users to be part of a virtual community. Current popular examples of these are Facebook, Twitter and for younger users, 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. NB: Many Social Network sites have age restrictions for membership e.g. Facebook's minimum age is 13 years old.

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

The school will control access to social networking sites, and consider how to educate pupils in their safe use.
Newsgroups will be blocked unless a specific use is approved.
Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
Pupils will use only moderated social networking sites, e.g. SuperClubs Plus
Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
Pupils will be advised to use nicknames and avatars when using social networking sites.

Staff are expected to manage their digital identity and portray themselves in a positive, professional and appropriate manner when posting or sharing content online. Staff should have privacy settings in place where appropriate and should check and review these on a regular basis.

Staff should not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any personal blogs or websites.

Staff should not add Pupils (past or present) as “Friends" on any Social Network site.

Staff should never post on behalf of, or refer to the school, pupils or parents on any social networking site, unless it is from the school’s official accounts and with the permission of the head teacher.

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. There is no such thing as private.

Instant Messaging:

Instant Messaging, e.g. MSN, Yahoo Messenger, is a popular communication tool with both adults and children. It provides an opportunity to communicate in real time using text, sound and video. It is not appropriate to use these tools in school.

NTLP Gmail provides its own filtered instant messaging and video chat service, which should be the only messaging service used in school, and then only used by pupils with adult permission. All ‘chat’ conversations are recorded and filtered by the same system that is used to filter the email. Inappropriate content in ‘chats’ will be flagged up to NT ICT automatically.

Virtual Learning Environment (VLE) / Learning Platform:

Pupils can communicate via the VLE, using email and instant chat. These forms of communication are filtered by North Tyneside.

Passwords are issued by the ICT Co-ordinator/School Business Manager and pupils are aware that these passwords should not be recorded in any form. All staff have the ability to reset passwords for all users at our school.

Pupils can access all tools on the VLE that are displayed when they log in.

Pupils receive regular e-safety reminded teaching them how to use these communication tools in a responsible way. This session is carried out by the Class Teacher and once completed reported back to the e-Safety coordinator.

Accounts are linked directly to our school’s SIMS data. Accounts are added or removed automatically by NTLP systems as data is uploaded to our SIMS systems.

Published content and the school web site

The school web site –http://www.marineparkfirst.co.uk/ - celebrates pupils’ work and promotes the school.

Staff or pupil personal contact information will not be published. The contact details given online should be the school office. The point of contact on the Web site is the school address, school e-mail and telephone number.

The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Video conferencing

Video chat (between NTLP users) is available through NTLP Gmail, using the video chat facility when a

webcam is available. Other free video conferencing software (such as Skype) is easily available. It can be a wonderful way to bring the outside into the classroom and establish links with schools or individuals in other places that might not be otherwise accessible for the children's learning.

Any use of video conferencing/video chats must only take place with the permission of a member of the senior leadership team (SLT). Any use of external video conferencing software (e.g. Skype) must not be done with a teacher's 'personal' account. It is good practice to create a separate account for school communications. Where possible, a discussion of some kind should take place with the 'caller' before the live conversation to ensure they know the expected audience of the call, the age of the children present, and what is appropriate for discussion in the call. This might be used when contacting an expert in their field to 'bring them in' to the classroom to enhance the children's learning.

An adult must always be present in the room when any video conferences/chats are taking place. The regulations for using webcams are similar to those for CCTV. This means that the area in which you are using the webcam must be well signposted and people must know the webcam is there before they enter the area, in order to consent being viewed in this way. Children should be consulted and adults would need to consent as well as the parents of all children involved.

In gaining consent, you must tell the person why the webcam is there, what you will use the images for, who might what to look at the images and what security measures are in place to protect access.

As children also have access to NTLP Google video chat outside of school, they must also be educated about safe, appropriate and acceptable use of these technologies, considering the following points:

- how, when and why they make use of it;
- ensuring an appropriate adult knows they are using it;
- never accepting a chat request from someone they do not know;
- reporting anything they find upsetting or inappropriate in a video chat to a trusted adult or by clicking the 'Report abuse' button on the NTLP main banner;
- protecting their personal information when using it. This may include not just what they say in a 'chat', but even the objects in the room around them which may inadvertently give away personal information they don't wish to share.

Use of digital media

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

- All staff and pupils instructed that full names and personal details should not be used on any digital media, particularly in association with photographs.
- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Group photographs rather than full-face photos of individual children are preferable.
- We ask all Parents/carers to provide written permission stating whether or not they can have their photograph taken and used within school or on the school website
- Pupil image file names will not refer to the pupil by name.
- All staff are instructed of the risks associated with publishing images, particularly in relation to use of personal Social Network sites.
- Our school ensures that photographs/videos are only taken using school equipment and only for school purposes. Staff are instructed that these images/videos are not to be stored on any personal computers, devices etc.

- We do not allow staff to store digital content on personal equipment.
- 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 are made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved. They are made aware of these dangers through e-safety lessons and training from outside agencies.
- Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.
- Staff sign an AUP informing them of the guidelines for safe practice relating to the use of digital media, as outlined in the schools' policy. These are monitored by our eSafety coordinator and SLT.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

6. Policy Decisions

Authorising Internet access

All staff must read and sign the "Staff Code of Conduct for ICT" before using any school ICT resource.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

At Key Stage 2, pupils accessing the internet are directly supervised by a member of staff.
Extended school provision accessing the internet are directly supervised by ASC staff on directed sites.

Parents will be given details of the acceptable use agreement that pupils have signed. This e-safety policy will be published on the school website and advice on safe use of the internet will be provided.

Any person not directly employed by the school will be asked to sign an "acceptable use of school ICT resources" before being allowed to access the internet from the school site.

7. Handling e-safety incidents

Our e-Safety Coordinator acts as first point of contact for any complaint. The Local Authority supplies the following flowchart to suggest appropriate action when dealing with eSafety incidents and in particular, social networking related incidents - Click here for Flowchart

Assessing risks

The school will take all reasonable precautions to ensure e-Safety and prevent access to inappropriate material. The school has completed a risk assessment which incorporates the Prevent Duty. This can be

reviewed in the Prevent Duty Policy. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Methods to identify, assess and minimise risks will be reviewed regularly. The SLT will ensure that the e-Safety policy is implemented and compliance with the policy monitored.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Incidents involving pupils

Incidents of cyberbullying are dealt with in accordance with our bullying and behaviour policy. Incidents related to child protection are dealt with in accordance with the school's child protection policy.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and reported to the Headteacher immediately (The Policy has a flowchart of responses to an incident of concern).

If an incident occurs involving a pupil, the member of staff in charge must seek the nearest member of staff so they can witness the misuse, protecting them any incident/allegation towards themselves.

The device where the incident took place (if in school) must be taken out of use until appropriate evidence can be captured to log the incident.

All staff are instructed of different types of eSafety incidents and are aware that they must report them to the above staff immediately.

Once incidents are reported to the above staff, a record must be made by the member of staff involved, which will then be filed in our eSafety log book which is incorporated within the Encrypted Electronic Incidents Log Documents.

One of the designated members of staff will inform how to deal with the incident.

If necessary the Local Authority will be informed of any misuse and parents will be informed.

Pupils and parents will be informed of consequences for pupils misusing the Internet. Parents and pupils will need to work in partnership with staff to resolve issues.

As with other safeguarding issues, there may be occasions when the other outside agencies must be contacted. Incidents of a criminal nature; i.e. threatening, intimidation or harassment then may then involve contact with the police for further advice (at the discretion of the headteacher).

Parents and pupils are given information about infringements in use and possible sanctions. Sanctions for

pupils include:

- informing parents or carers;
- removal of Internet or computer access for a period of time.
- referral to LA / Police.

Incidents involving staff

Any incident involving staff misuse must be referred immediately to the Headteacher.

It is fully recognised that an authorised staff user may accidentally breach this policy whilst acting in good faith and in the course of their duties. If a member of staff suspects this may be the case they must notify the Headteacher or nominated e-safety coordinator IMMEDIATELY so that action can be taken to prevent or minimise damage.

Any authorised user who commits a breach of any school policy as a result of unauthorised use of electronic media may face disciplinary procedures. If the school discovers that a member of staff has committed a criminal offence or has been party to the commission of one as a result of unauthorised use of electronic media the police will be contacted immediately. The school will in no way indemnify a member of staff who has incurred any liability as a result of unauthorised use of electronic media. The school will seek financial redress from an authorised user whose misuse of electronic media causes the school to suffer a loss.

Incidents involving other adults (e.g. parents)

Any incident affecting the school but involving other adults out of school must be referred immediately to the Headteacher.

Where possible, evidence should be collected immediately and individuals concerned may be contacted by the Headteacher to discuss the incident.

If necessary the Local Authority will be informed of any misuse. Incidents of a criminal nature; i.e. threatening, intimidation or harassment then may then involve contact with the police for further advice (at the discretion of the Headteacher).

8. Communications Policy

Introducing the e-safety policy to pupils

E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.

Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

A programme of training in e-Safety has been developed, based on the materials from CEOP, Hectors world and sites recommended by North Tyneside ICT Team.

E-Safety training will be embedded within the Computing scheme of work and the Personal Social and Health Education (PSHE) curriculum.

Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its importance explained.

Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

Staff will always use a child friendly safe search engine when accessing the web with pupils.

The school will liaise with the LA as part of the ICT SLA to provide effective support to staff. For example, training on e-safety for staff was provided on a training day in January 2014.

Enlisting parents' and carers' support

Parents and carers attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

The school will maintain a list of e-safety resources for parents/carers.

The school will be made aware of the pupil agreement when they register their child with the school.

The school will liaise with the LA as part of the ICT SLA to provide effective support to parents and carers. For example, a series of drop in workshops were held to inform parents to coincide with parents evening in autumn 2013 and have planned to repeat this in 2016.

9. Standards and inspection

Staff will regularly remind children of eSafety rules and any incidents that occur are closely monitored by the eSafety coordinator.

If we feel incidents are occurring and our eSafety policy is not having the desired effect we will seek advice from the North Tyneside ICT team.

Each incident that takes place will be reviewed by the eSafety coordinator and action will be taken immediately.

Incidents will be analysed to see if there is a recurring pattern e.g. specific days, times, classes, individual children etc. If a pattern does occur they will be addressed by targeted work with specific classes, groups, children, parents.

Staff, parents/carers, pupils and governors are informed of changes to policy and practice via newsletters, meetings and training sessions.

AUPs are reviewed annually and they will be updated to include current trends and new technologies, whenever necessary.

10. Appendices

Appendix 1: Internet use - Possible teaching and learning activities

Activities	**Key e-safety issues**	**Relevant websites**
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. bookmarks, the school VLE
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids Yahooligans Googel safe search Kidsclick dinosearch
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs Plus.	NTLP Gmail and other Google apps.
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted. Pupils' work should only be published on „moderated sites" and by the school administrator.	Making the News SuperClubs Plus Headline History North Tyneside Learning platform Cluster Microsites National Education Network Gallery
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name. Staff must ensure that published images do not breach copyright laws.	Making the News SuperClubs Plus Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art Cluster Microsites National Education Network Gallery
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Plus FlashMeeting
Audio and video conferencing to gather information and share pupils" work.	Pupils should be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.	FlashMeeting National Archives "On-Line" Global Leap JANET Videoconferencing

		Advisory Service (JVCS)

Marine Park First School

Key Stage 2 eSafety Rules

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use my own school NTLP email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will take great care and check with my teacher or another responsible adult before giving out my own personal details. These may be my name, age, phone number, school, home address, user-names, passwords or anything else that could be used to identify me.
- ✓ I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- ✓ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- ✓ 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.

Marine Park First School

Foundation Stage and Key Stage 1 eSafety Rules

Think then Click - These rules help us to stay safe when using a computer		
	We only use the Internet when an adult is with us	
	We can click on the buttons or links when we know what they do.	
	We can search the Internet when an adult is with us.	
	We always ask if we get lost on the Internet.	
	We can send and open emails together.	
	We can write polite and friendly emails to people that we know.	
	We always ask for help if we have a problem or feel worried on the Internet	

Pupil's Agreement

- I have read and I understand the school e-Safety Rules.
- I know that network and Internet access may be monitored.
- Please sign in the box below:

Adult Acceptable Use Policy

All adults working in school

All adults working with ICT equipment in Marine Park First School must ensure that they have read and agree to abide by the Acceptable User Policy.

The computer system is owned by the school, and may be used by students to further their education and by staff to enhance their professional activities including teaching, research, administration and management.
The school's Internet Access Policy has been drawn up to protect all parties - the pupils, the staff and the school.
The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.
Staff and students requesting Internet access must accept and comply with the following guidelines.

For personal use:
Internet access in school is filtered to prevent the viewing and downloading of inappropriate material. Do not attempt to access inappropriate sites. Downloading some material is illegal and the police or other authorities will be called to investigate such use.

Viruses are a serious threat. Do not introduce devices (memory sticks etc) into the system without first having checked for viruses.

Please respect other people's material and do not corrupt, interfere with or destroy them. Do not open other people's files unless they are in the teachers shared folder.

Your username and password are unique to you so do not give them to anyone else. Always remember to log out and close the browser when the session has finished.

Do not release or in any way make available personal details of any colleague or pupil (phone numbers, fax numbers or personal e-mail addresses) over the Internet.

When working with SIMS or any other personal data ensure that the data is secure.

Reproducing copyright materials without first getting permission from the owner is an offence. Please get the required permission before use and where appropriate acknowledge sources.

Do not take digital photographs or videos without permission. This includes personal digital cameras or mobile phone cameras. The use of personal digital cameras and/or mobile phones to take photographs is permitted with permission. Images however must be transferred to school network for storage and deleted from personal property.

Use of school Internet access for business, profit, advertising or political purposes is strictly forbidden.
Do not leave laptop computers, iPads or any other easily transportable ICT equipment unattended at any time.

Personal E-mail

- Follow school guidelines contained in the ICT policy for the use of e-mail.
- Observe *netiquette* on all occasions. E-mail should not be considered a private medium of communication.

- Do not include offensive or abusive language in your messages or any language which could be considered defamatory, obscene, menacing or illegal. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority.
- Make sure nothing in the messages could be interpreted as libelous.
- Do not send any message which is likely to cause annoyance, inconvenience or needless anxiety.
- Do not send any unsolicited promotional or advertising material nor any chain letters or pyramid selling schemes.

When using the Internet or e-mail with children

- Teach children of the rules for using the Internet or e-mail and the implications of misuse.
- Watch for accidental access to inappropriate materials and report the offending site to the School nominated person for Internet Safety, Mr. Easton.
- Check before publishing children's work on the school web site; make sure that children cannot be identified.
- Report any breaches of the school's Internet policy to the designated person, Mr. Easton
- Try to provide pupils with direct links embedded into 'pages' in a document, NTLP, or interactive whiteboard resource etc.
- If you do need to undertake Internet searches (including Internet image searches), rehearse before you use in class. Think about search terms. Even the most innocuous term can bring up adult material.
- Use child-friendly search engines with younger pupils. Older young people will use a variety of search engines at home. You are a role model for them so need to model good use of a search engine. Look for opportunities to teach young people how to use search engines effectively.
- When checking out web content make sure you are not displaying it on the interactive whiteboard or via a projector – research away from pupils.
- Watch YouTube (or any) videos before you use them in the classroom.
- If you use a YouTube (or any) videos, find out how to embed it using the 'Source' rather than a page link, as that exposes pupils to other content.
- If you cut and paste or save content from the Internet or other peoples files make sure you remove the hyperlinks embedded in the text, or attached to images.
- If you want to use a clip download it (if legal & copyright allows), it might not be there next time you look for it.
- You need to be a good role model for copyright. Make sure you use multimedia resources appropriately, don't just 'grab stuff' off the Internet. Use the copyright images from the NEN, LGfL or other sites your school / LA has advised you of. You cannot show DVDs in school, although it is safe to use film trailers. But, make sure you download the right version, as there are can be more than one film trailer, including trailers for 'adult versions' of blockbusters.
- Think very carefully about sending or posting 'sexy' photos or text to your friends ("sexting") as they can be forwarded with potential very embarrassing outcomes or even cyber-bullying.

When using the emerging/mobile technologies (digital cameras, mobile phones, video conference)

- Named images of pupils (e.g. photographs, videos, web broadcasting, TV presentations, web pages etc.) must not be published under any circumstances other than for display and use in school.
- Written permission from parents or carers will be obtained by the school office before photographs of pupils are taken.
- The development of technologies such as videoconferencing will be monitored and evaluated by staff.

- Permission to engage in video conferencing activities must be approved by person responsible for internet safety and permission sought from the parents and carers of the children involved.

Safe use of email - Guidelines for staff

- The following guidelines will help schools implement the use of e-mail and apply to both staff and pupils.
- Do not attempt to give all pupils e-mail access straight away. Provide training and awareness of good practice, and plan for its implementation.
- Take into account the age of the pupil and their ability to use e-mail. Consider the need for individual addresses as opposed to class or group addresses and the ability of the pupil to understand the potential dangers of using e-mail to communicate with strangers.
- Pupils and staff must understand that their e-mail address can be picked up from a sent e-mail. It is very useful to have a number of general school e-mail addresses that can be given out in some cases.
- Pupils must be taught to keep their e-mail address secure and only send messages to people or organizations they can trust.
- They should not give their e-mail address to strangers nor should they reply to unsolicited e-mails. If they receive abusive or offensive e-mails they must not reply to them and should report such occurrences to their teacher.
- Pupils should not give details in e-mails, or in any other way on the Internet, that could identify their home address or phone number/mobile number.
- Sensitive or confidential information must not be sent by e-mail over the Internet. This is considered to be about as secure as sending an open postcard.
- Pupils must be advised never to meet with anyone with whom they have been communicating via the Internet/e-mail unless they first discuss this with an adult. The issue of potential 'electronic stranger danger' should be discussed with the pupils.
- Ensure all staff and pupils are aware that e-mails sent and received via school computers may be inspected at any time.
- Pupils and staff should be aware that e-mails from the school present an image of the school to recipients and therefore should not contain anything that would cause offence or present the school or user in a bad light.

Examples of good practice when using email

As the use of email continues to grow, there is a need to identify good practice. The suggestions below are a few examples of good practice.

- Ensure pupils and teachers are aware of who is responsible for monitoring the use of email.
- Do not forward chain letters to anyone else, and report them to the appropriate person.
- Know how to deal with and avoid receiving junk mail and unsolicited mail
- Do not impersonate anyone else using e-mail
- Do not use e-mail to send comments or information that is defamatory or libelous, or use e-mail as a means of harassment, intimidation or annoyance to anyone else. The sender of an e-mail should only send messages the contents of which they would be happy to be receive or have read out in court. E-mail messages are admissible as evidence.
- Do not reply to pestering, offensive or suggestive e-mails - pupils should report such occurrences to a teacher or appropriate adult.

- There is a growing instance of computer viruses being sent by email, often innocently. If you think you have received a virus, delete the email without opening it and report it to the teacher or appropriate adult.

Advice for use of social media

Social networking sites are great ways to stay in touch with friends and share photographs, comments or even play online applications. However, they are also designed to enable advertisers to target you and entice you into buying goods and services based on the 'profile' information you reveal. Be web savvy!

- Social networking sites, such as Facebook, have a range of privacy settings. These are often set-up to 'expose' your details to everyone - anyone could find you through a search of the networking site or even through a Google search. So, it is important to change your settings to "Just Friends" so that your details, photographs, location, etc., can only be seen by your invited friends.
- Have a neutral picture of yourself as your profile image. Don't post potentially embarrassing material.
- You do not need to accept friendship requests. Reject or ignore unless you know the person or want to accept them. Be prepared that you may be bombarded with friendship requests or 'suggestions' from people you do not know.
- Choose your social networking friends carefully and ask about their privacy controls.
- Do not accept 'friendship requests' on social networking or messaging sites from students, pupils or young people (or their parents) that you work with. Remember ex-pupils may still have friends at your school.
- Exercise caution – for example in Facebook if you write on a friends 'wall' all their friends can see your comment – even if they are not your friend.
- There is a separate privacy setting for Facebook groups & networks, you might have your profile set to private, but not for groups & networks. If you join a group or network everyone in the group or network will be able to see your profile.
- If you have younger family members on your social networking group who are friends with your students or pupils be aware that posts that you write will be visible to them.
- If you wish to set up a social networking site for a school project create a new user profile for this, do not use your own profile.
- If you or a friend are 'tagged' in an online photo album (Facebook, Flickr or similar) the whole photo album will be visible to their friends, your friends and anyone else tagged in the same album.
- You do not have to be friends with someone to be tagged in their photo album.
- If you are tagged in a photo you can remove the tag, but not the photo.
- Photo sharing web sites may not have privacy set as default.
- Your friends may take and post photos you are not happy about. You need to speak to them first, rather than contacting a web site. If you are over 18 the web site will only look into issues that contravene their terms and conditions.
- Use location settings wisely. Many social networking and online applications disclose your location. Where this is specifically linked to your identity it will, within a couple of days have disclosed where you live and when you are not at home.
- "I'm attending..." – there are social networking groups to bring together people sharing experiences, such as attending festivals and conferences. Great idea, but don't forget this advertises when you will not be at home.
- Be careful not to leave your Facebook account logged-in in a shared area / household because someone could then leave status messages that may compromise or embarrass you. This is called Frape (Facebook Rape), and can be a form of cyber-bullying.

- If you think someone is impersonating you on Facebook or similar, report it. Impersonation usually breaches the terms and conditions – you will need to know the specific URL or user name, sites cannot work from a hunch.
- Think before you post! Once something is on the internet, even if you remove it, the chances are it has already been snapshotted by a 'web crawler' and it will always be there. Archives of web content are stored on sites like the WayBackMachine.
- Think about your internet use, adults are just as likely to get hooked on social networking, searching or games. Be aware of addictive behaviour.
- You will not be able to remove yourself completely from the Internet. 192.com has all the English electoral rolls and for as little as £9.99 your personal information can easily be found by a stranger.

Phone hints and tips

- Don't give out your mobile number or home number to students or pupils.
- If you have a Bluetooth phone do you know if Bluetooth is turned on or off? If it is on is there a password? Open un-passworded Bluetooth means anyone else with Bluetooth in range can read the content of your phone or device.
- Many hand held games consoles have wireless and Bluetooth and can be used to make contact from 'stranger' devices within range.
- Lock your mobile. Set a pin number or password for your mobile phone. With access to email, social networking and contacts an unlocked mobile phone can put your identity, and others, at risk.

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with **Mr. Easton,** the Headteacher.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be safe and responsible users of the internet and other digital technologies.
- that school ICT systems and users are protected from accidental or deliberate misuse.
- the school will try to ensure that staff and volunteers will have good access to ICT to enhance their work and improve opportunities for learners and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

- I understand that I must use school ICT systems in a responsible way, to minimise the risk to my safety or to the safety and security of the ICT systems and other users.
- I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school may monitor my use of its ICT systems including email and other digital communications technologies.
- I understand that this agreement also apply to use of school ICT systems out of school (e.g. laptops, email, Learning Platform etc).
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and guidelines set down by the school.
- I will keep my usernames and passwords private and will not try to use anyone else's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, to the appropriate person in school.
- I understand that it is my responsibility to report any known misuses of technology, including the unacceptable behaviours of others.
- I will be an active participant in e-safety education, taking personal responsibility for my awareness of the opportunities and risks posed by new technologies.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, delete or otherwise alter any other user's files, without their permission.
- I will communicate with others in a professional manner. I will not use any communications device, to bully or harass others in any form.
- I will ensure that when I take or publish images of pupils or parents/colleagues, I will do so with their permission and in accordance with the school's policy.
- I will only use school cameras, not use my personal equipment to record these images, unless I have permission to do so, following school policy.
- Where these images are published (e.g. on the school Learning Platform) it will not be possible to identify pupils by name, or other personal information.
- I will not use chat and social networking sites in school, other than the Learning Platform blog facility/gmail facility or school accounts that have been approved by the Headteacher.

- I will only communicate with pupils and parents / carers using official school systems, not personal mobiles and in a professional manner.
- I will not share any personal information with a pupil (including personal phone numbers or email address). Nor will I request or respond to any personal information from a young person unless it is appropriate as part of my professional role.
- I will not engage in any on-line activity that may compromise my professional responsibilities or bring the school into disrepute

The school and the local authority have the responsibility to provide safe and secure access to technologies:

- I will only use password protected memory sticks which have been provided by the school to store sensitive pupil information such as pupil data and photographs.
- I will protect my passwords and personal network logins, and will log off the network when leaving workstations, laptops unattended.
- I will ensure that when teaching, all classes log of before leaving the ICT suite.
- I will ensure that laptops are securely locked away at the end of the day if being left on the premises or if being taken home, are never left unattended in vehicles etc.
- I will not use personal email addresses on the school ICT systems – only ntlp accounts should be used.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any material which is illegal or inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering /security systems intended to prevent access to such materials.
- Unless I have permission, I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on school systems, nor will I try to alter computer settings, unless this has been agreed by the Headteacher.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where personal data is electronically transferred outside the secure school Citrix network (on the office computer) it must be encrypted.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- When I use my personal hand held / external devices in school (PDAs / laptops / mobile phones / USB devices etc), I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that when connecting these devices to school ICT systems, they are protected by up to date anti-virus software and are free from viruses. (Visitors)

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action and in the event of illegal activities, the involvement of the police.

- I have read and understand the above and agree to use the school ICT systems both in and out of school and my own devices (in school and when carrying out communications related to the school) within these guidelines.

When I leave the School I understand that

- My Email account will be disabled. School technical administrators may keep access to the account by forwarding mail to an alternative account. This will help address any ongoing issues, projects that need to be completed, outstanding actions etc.
- My Network access password in the computer suite will be disabled. Prior to this all files must be inspected by the Headteacher prior to making them available to other year group users.
- My laptop files must be inspected by the Headteacher/network manager. They will be thoroughly checked for inappropriate content, malware, illegal copies etc. prior to being made available to other users.
- Files, programs, data must not be taken away from the school without explicit permission from the Headteacher
- Images of pupils away from the school when they cease to be employed by the school.
- All portable devices including memory sticks must be returned to the Headteacher.

The use of mobile telephones for staff

- I understand that staff are allowed to bring in mobile phones for their own personal use. However, they must be kept in lockers/handbags at all times and are not allowed to be used when children are present or in the playground at anytime.
- If a mobile phone is to be used during non-teaching time, i.e.at breaktime or lunchtime, calls should be made away from any area used by the children
- I should ensure that there is no inappropriate or illegal content on the device.
- Mobile phone technology may not be used to take photographs anywhere within the school grounds.
- I understand that staff should only contact a parent/carer on a school telephone.
- When children undertake a school trip or journey, personal mobile phone use by adult leaders should be limited to contact with the school office or venues being visited, except in emergencies.

Use of Mobile Phones and Cameras for Volunteers/Students

- Upon my initial visit as a volunteers/students I have been given information informing me that I am not permitted to use personal mobile phones or digital cameras on the premises. If I wish to make or take an emergency call during school teaching time, I may use either the main school office.

Name _____

Signed _____ Date _____

Passwords and Password Security

Passwords

Always use your own personal passwords to access computer based services

Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures

Staff should change temporary passwords at first logon

Change passwords whenever there is any indication of possible system or password compromise.

Do not record passwords or encryption keys on paper or in an unprotected file

Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished

Passwords must contain a minimum of six characters and be difficult to guess and change annually. Protected data accessed through Citrix users must be changed every term.

User ID and passwords for staff and pupils who have left the School are removed from the system within ***4 weeks.*** *(see starters and leavers guidance)*

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security

Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) log-in username. From ***Year 3*** they are also expected to use a personal password for the Learning Platform and keep it private.

Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others

Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the school network is ***6.30pm***

Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer)

In our school, all ICT password policies are the responsibility of the Headteacher and e-safety coordinator and all staff and pupils are expected to comply with the policies at all times

Starters and Leavers Policy

What to Do When a Teacher/ Staff member leaves

The purpose of this document is to:

Help ensure that a school's data and resources remain secure as personnel leave the organisation

Help reduce the opportunity for misplaced or malicious allegations.

Adults who work in schools may have access to a range of important and sensitive information including images and personal details of colleagues and learners and it is essential that the integrity of the school's systems and files remain intact when colleagues leave the school.

Email – disable password. School technical administrators will need to keep access to the account by forwarding mail to an alternative account. This will help address any ongoing issues, projects that need to be completed, outstanding actions etc.

Network – change access password. Delete files or inspect prior to making them available to other users.

Secure areas – ensure key codes are changed and all keys retrieved.

Portable devices – need to be thoroughly checked for inappropriate content, malware, illegal copies etc. prior to being made available to other users.

Learning platform – account disabled but not deleted. This will ensure all useful documents can continue to be used by the school.

Files, programs, data - ensure none are taken away from the school if the copyright is only for the institution.

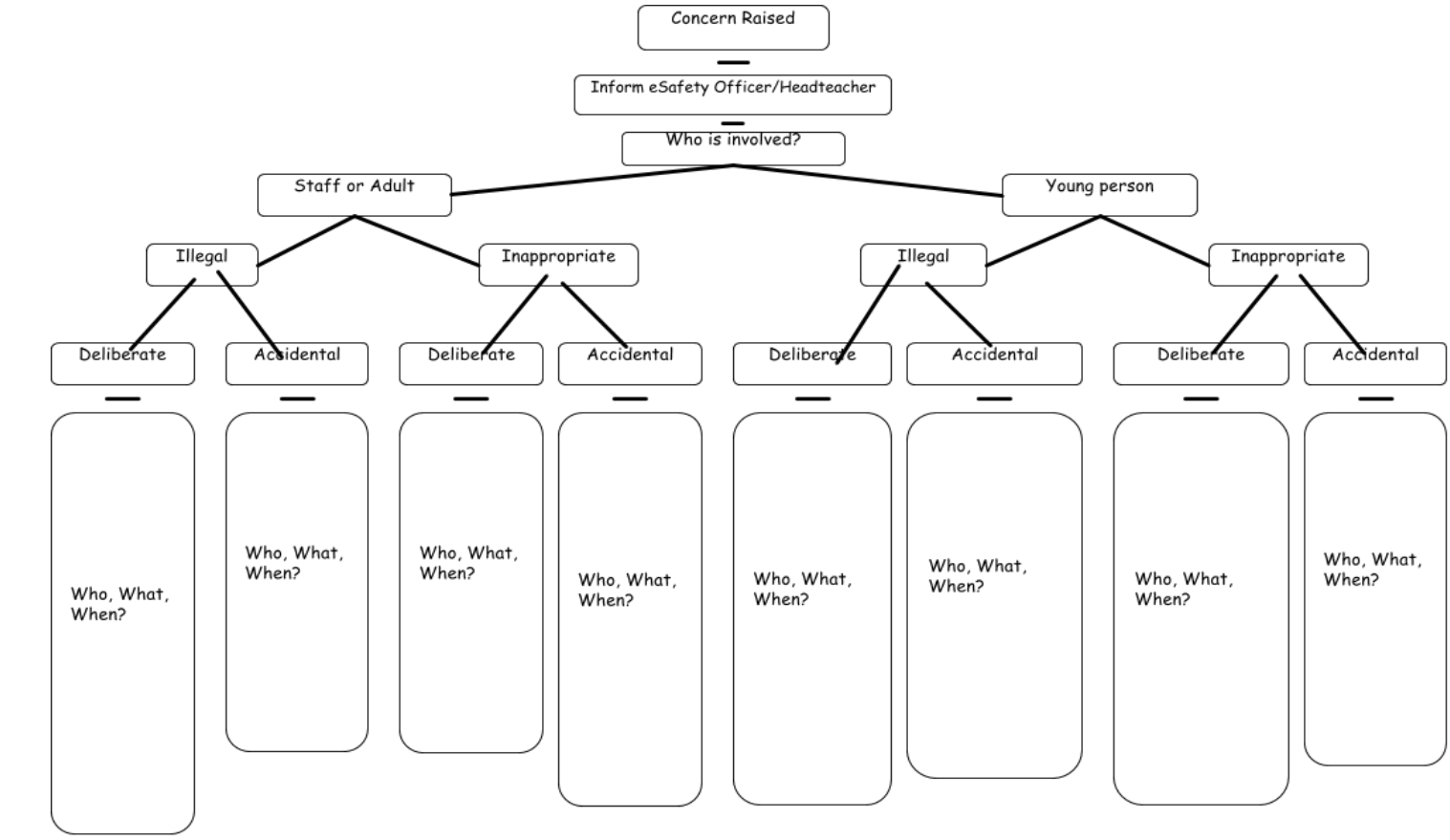
Images – no teacher can take images of pupils away from the school when they cease to be employed by the school.

What to Do When a Pupil Leaves

Network – remove log-in from system. Delete files or inspect prior to making them available to other users.

Learning platform – account disabled but not deleted. (Details to be sent to the Learning Platform Coordinator), Email – disable password.

Dealing with an eSafety Incident



MARINE PARK FIRST SCHOOL - Equality Impact Assessment

1. Name of the change, strategy, project or policy:	**E- SAFETY POLICY**
2. Name of person(s) completing this form:	**S. EASTON**

3. Has the policy/practice been assessed to consider any potential impact on the equality groups?

Yes – The key principles of this policy have been formulated to outline expectations of all members of the school with respect to the use of ICT-based technologies in order to safeguard and protect all children and staff. In formulating this policy no negative impact on any equality group has been identified.
The School will fulfil its obligations to equality by approaching its practices in E-Safety in a fair and consistent manner.

Where potential impact has been identified, please complete questions 5-9. If none is identified, please proceed to question 10.

4. Equality Target Group (circle):	Negative impact – it could disadvantage	Reason
Race Religion/belief Disability Gender Gender Reassignment Sexual Orientation Age Pregnancy/Maternity Marriage & Civil Partnerships		

5.	Yes	No
a) Is the impact legal/lawful? Seek advice from your School link HR Advisor if necessary.		
b) Is the impact intended?		

6. Does this action/policy/procedure attempt to meet the aims of the public sector equality duty? (this should feed into your Single equality scheme & action plan)	Yes, No, N/A	If yes, please provide details
Eliminate unlawful discrimination, harassment and victimisation		
Advance equality of opportunity between different equality groups		
Foster good relations between different equality groups		

7. If you have identified any negative impact, have you identified any ways of avoiding or minimising it?

8. Is it possible to consider a different policy/strategy/action, which still achieves your aim, but avoids any negative impact on people?

9. In light of all the information detailed in this form; what practical actions would you take to reduce or remove any negative impact?

PART B) To be completed when assessment and consultation has been carried out

10.a) As a result of the assessment and consultation completed in Part A above, state whether there will need to be any changes made to the policy, project or planned action. **10.b)** As a result of this assessment and consultation, does the school need to commission specific research on this issue or carry out monitoring/data collection?
No.

11. Have you set up a monitoring/evaluation/review process to check the successful implementation of the policy, project or change?	Yes	**x**	No	

The Governing Body will receive information periodically from the ICT Curriculum Coordinator and Headteacher regarding E-Safety. This policy will be kept under periodic review.