Duke Street Primary School

eSafety Policy

September 2014

Contents

Developing and Reviewing this Policy

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

Mrs Nicola Worth (Computing Subject Leader)

Mr Andrew Kidd (Head Teacher)

Mr Nigel Kirkham (Lancashire ICT advisor)

Duke Street School Council - Golden Rules for Staying Safe online

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

Policy Created - Date:

The implementation of this policy will be monitored by: Nicola Worth and Andrew Kidd.

This policy will be reviewed as appropriate by

Mrs Nicola Worth (Computing Subject Leader)

Mr Andrew Kidd (Head Teacher)

Approved by ....(Head Teacher) Date: ....

Approved by ....(Governor) Date: ....

1. Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective eSafety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our eSafety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings.

2. Vision Statement for eSafety.

- Duke Street's vision is for all the school community to be responsible, competent, confident and creative users of information and communication technology.
- At Duke Street we use technology when appropriate to enhance the learning experience for our children and to support the daily organisation and administration tasks carried out by school staff.
- Following the objectives in the Computing National Curriculum, we will teach the children to:

  "*use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact*"

- Our eSafety Policy defines what we consider to be acceptable and unacceptable behaviour regarding the uses of technology in school and the sanctions or procedures to be followed should breaches of security occur. It is communicated to staff, governors, pupils and parents and is updated in light of the introduction of new technologies or incidents.

3. The School's eSafety Champion.

Our eSafety Champion is Mrs Nicola Worth

The role of the eSafety Champion in our school includes:

- promoting and monitoring the safe use of ICT within school
- ensuring all children are educated in the safe use of ICT, within and out of the school environment
- monitoring and reviewing the eSafety policy, and Acceptable Use Policies
- keep 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).
- training staff members on the safe use of technology as necessary, ensuring all staff are aware of reporting procedures in the event of an eSafety incident occurring.
- being the school's point of contact for eSafety-related issues and incidents
- liaising with the school's DSP where necessary in the case of child protection
- ensuring the eSafety Incident Log is appropriately maintained and regularly reviewed

- arranging or providing eSafety advice/training for parents/carers/governors as necessary

4. Policies and practices

E-safety is taken seriously at Duke Street. Any breaches of policy must be reported directly to the Headteacher for investigation.
This eSafety policy should be read in conjunction with the following other related policies and documents:
ICT Policy
Anti-bullying
Child Protection
Safeguarding
Behaviour Policy
Staff Handbook

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

Our school ensures that data is appropriately managed both within and outside the school in the following ways:

- The Head teacher has ultimate responsibility for all the information that is held in school, and is in charge of managing all data and information, both within and outside the school environment.
- Relevant staff will be shown the location of data necessary to their position during the induction process.
- All staff with access to personal data are made aware of their legal responsibilities as part of the induction process.
- School's equipment, including teacher laptops, must only be used for school purposes and do not contain personal information e.g. personal images, personal financial details, music downloads, personal software. Computers are accessed via a safe username and password and it is the responsibility of the individual to keep this secure at all times. Any breaches in security must be reported immediately to Nicola Worth or Andrew Kidd.

- School equipment must not be used, for example for online gambling, dating websites, home shopping, booking holidays, and social networking BOTH at home and in school.
- Staff are aware of the school's procedures (eSafety) for disposing of sensitive data, e.g. shredding hard copies, deleting digital information, deleting email accounts, IEP, PIPs, SATs information and know the person responsible should there be any queries.
- The school's policy for removal of sensitive data prior to disposal or repair of equipment is carried out by a registered company. http://www.uk-computer-recycling.co.uk/services/data_destruction.html
- School data must NOT be stored on personal equipment, e.g. home computer or mobile phone.

4.2 Use of mobile devices

In our school we recognise the use of mobile devices offers a range of opportunities to extend children's learning. However, the following statements must be considered when using these devices:

- All devices with 3G/4G wireless connections can access unfiltered internet content. Therefore, this facility must be turned off before children use such devices.
- Any devices that use the school network must contain up-to-date virus software.
- Portable USB devices are permitted to be used, as the school has up-to-date Anti-Virus software. However, staff must ensure that personal computers that the devices are also used with have sufficient Anti-Virus protection.
- Staff are permitted to bring in personal mobile devices, however these must be kept securely. These must only be used appropriately for personal reasons, for example not making or receiving personal phone calls when children are present. In addition, phones should only be used by staff outside working hours, except when absolutely necessary. Any data captured on such devices for professional reasons, for example a voice recording during a lesson, must be transferred onto a school computer and deleted immediately from the mobile device. It is not acceptable for staff to take pictures on mobile phones.
- Pupils may on occasion need to bring a mobile phone into school. However, they must leave it at the school office before registration, and may collect it at the end of the day. All staff can confiscate any personal mobile devices that are deemed valuable and desirable, and will arrange for them to be kept securely in the office.
- iPads for pupil use are kept securely in a locked trolley and the key is kept by Mrs Worth / Mr Kidd. Passwords protect the children from being downloading any new APPs.
- Each iPad has its own Apple account and email so content is purchased to comply with Apple Terms and Conditions.

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.

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

- As photographs and video of pupils and staff are regarded as personal data in terms of The Data Protection Act (1998), we ensure we have written permission for their use from the individual and/or their parents or carers. This information is collected when a child starts school in reception or on transition from another school. We also ask for a new one to be signed on transition from KS1 to KS2. This will enable the consent form to be updated with any relevant changes. An up-to-date list is obtainable from the office.

- No names will be attached to photographs on the website or in the local media without the permission of the person involved and no children's names will be attached to photographs on the school website.
- Photographs and videos must only be taken on school equipment and must not be taken off the school premises.
- Parents/carers, who have been invited to attend school events, are allowed to take videos and photographs. They are made aware that these must only be for personal use in advance.
- Training has taken place to ensure that staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites.
- When taking photographs/video, staff must ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted.
- Publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved is an offence.
- Permission is gained via the consent form to allow us to retain images of children for use in school after a child has left.
- Images of children taken by staff are to be taken using a school iPad, iPod or school digital camera with a school SD card. These images need to be put onto the secure school server on a regular basis and then deleted from the portable device. The ICT Technician is able to do this on request.

4.4 Communication Technologies

Email

In our school the following statements reflect our practice in the use of email.

- All users have access to the Lancashire Grid for Learning service as the preferred school e-mail system. However, staff can choose to have any school based emails sent to their personal email address.
- Children are not permitted to access personal email accounts in the school environment. For the purpose of teaching 'Electronic Communication' or communicating with other children, for example pen pals, children may use the pupil accounts set up on the LGfL service whilst supervised. These accounts can be monitored easily by the Computing Subject Leader. Each pupil should be assigned a number e.g. pupil1, which they should continue to use for Electronic Communication, with adult supervision. e.g child5nhw@dukestreet-pri.lancs.sch.uk
- The Lancashire Grid for Learning filtering service should reduce the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of SPAM should be reported to the Westfield Centre.
- All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.
- 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 users are 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.

Social Networking

Social networking sites (i.e. Facebook, Twitter. Instagram, Tumblr etc.) are becoming increasingly popular amongst the adult population and young people. However, many sites do have age restriction policies (ref: COPPA - Children's Online Privacy Protection Rule) 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 anyone providing false information is violating the site 'Statements of rights'. For this reason, we would actively discourage pupils in our school using any social networking sites where these restrictions apply.

These communication tools are, by default, 'blocked' through the internet filtering system for direct use in Lancashire schools. However, comments made outside school on these sites may contravene confidentiality or bring the school or staff into disrepute.

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

- Staff 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.
- Pupils must not be added as friends on any Social Network site.
- Whatever means of communication staff use they should always conduct themselves in a professional manner.

Web sites and other online publications

In our school the following statements outline what we consider to be acceptable and unacceptable use of Websites and other online publications:

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Web site should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.
- Downloadable materials must be in a read-only format (e.g. PDF) where necessary, to prevent content being manipulated and potentially re distributed without the school's consent.

4.5 Acceptable Use Policy (AUP)

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

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

The school has the following AUP's in place (see appendices):
ICT AUP – Staff and Governor Agreement
ICT AUP – Students, Supply Teachers, Visitors, Guests etc, Agreement
ICT AUP – Childrens Agreement

Mrs Nicholls (School Bursar) is responsible for making sure all supply teachers and students that will be using a school computer, read and sign the appropriate AUP.

4.6 Dealing with incidents

At Duke Street we take any incident seriously and have a number of different ways of dealing with it depending on the severity or nature of the incident. Incidents are logged and these are regularly monitored and audited by the eSafety Champion and if necessary other key members of staff involved in Child Protection. It is likely that our school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and actions are proportionate to the offence. Some examples of inappropriate incidents are listed below with suggested sanctions.

Incident	**Procedure and Sanctions**
Accidental access to inappropriate materials	• Minimise the webpage/turn the monitor off/ • Tell a trusted adult. • Enter the details in the Incident Log and report to LGfL filtering services if necessary. • Persistent „accidental" offenders may need further disciplinary action.
Using other people's logins and passwords maliciously.	• Inform SLT or designated eSafety Champion. • 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
Deliberate searching for inappropriate materials.	
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate way.	

	with Behaviour Policy. • Consider parent/carer involvement.

Where staff are suspected of contravening the AUP, this should be reported to the Headteacher who will take appropriate steps in accordance with the school's discipline policy.

Duke Street uses a holistic approach to eSafety, and as such all staff are responsible for dealing with eSafety incidents appropriately at class level. The eSafety champion should be notified of any eSafety incidents, who will then liaise with the Headteacher as appropriate.

The eSafety log book will be kept securely in the Headteacher's office. This will be monitored regularly, with action plans put in place as necessary to avoid further incidents where possible. An example Incident Log can be found in the appendices.

The 'Lancashire eSafety Incident/Escalation Procedures' document will be followed (see Appendix) as a framework for responding to incidents.

5. Infrastructure and technology

We are lucky to have excellent facilities for ICT at Duke Street. They range from iPads to fixed desktop machines and classroom teaching computers. We can facilitate wireless technologies which enables us to use different devices at different times in different locations. We aim to make the infrastructure/network as safe and secure as possible by using the following measures:

- We subscribe to Lancashire grid for Learning/CLEO Broadband Service which provides us with a high level filtering service and Sophos Anti-Virus software.
- EYFS and Key Stage1 pupils have a class login, individual logins in key stage 2, to access desktops, and these are monitored by the class teacher and Computing Subject Leader/eSafety Champion. Children are supervised when using the equipment.
- Staff have their own logins which are password protected. This is monitored by the eSafety Champion.
- Only approved devices are allowed to use the wireless system. The network key is known by the eSafety Champion/Computing Subject Leader/ ICT Technician
- All software is legally owned with licences provided.

Managing the network and technical support:

- The network is managed and technical support provided by ICT in Education.
- Servers are located in a secure cupboard where there is no pupil access.
- All wireless devices have had their security enabled.
- The technician is responsible for managing the security of the curriculum school network and the
- Westfield Centre manages the security of the office network.
- Computers are regularly updated with critical software updates/patches by the technician.
- Breaches of security must be reported immediately to the Headteacher or Computing subject leader.
- Technical support providers are made aware of our schools requirements / standards regarding eSafety.
- It is the Computing subject leader's responsibility to liaise with/manage the technical support staff.

Pupil Access:

Pupils will only have supervised access to the internet. No access will be allowed during playtime or lunchtime. Pupils will only be allowed access when a positive consent form has been returned. An up to-date list is available from the school office.

6. Education and Training

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

The three main areas of eSafety risk (as mentioned by OFSTED, 2014) that your school needs to be aware of and consider are:

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

	• Sexting (sending and receiving of personally intimate images). • Copyright (little care or consideration for intellectual property and ownership – such as music and film).

(Ofsted, 2014, Inspecting eSafety – guidance document)

6.1 eSafety across the curriculum

The new Computing Curriculum 2013 states that children need to:

> *use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.*

At Duke Street we want the children to be active in the role of staying safe online. Our School Council children have contributed in writing the 'Golden Rules for Staying Safe online'. We have 2 versions of these rules (KS1 and KS2). (See Appendices)

As part of the new ICT (computing) curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, our digital footprint and cyber bullying.

eSafety is taught in all curriculum areas where relevant, in particular the strands of Digital Literacy. The school also participates in the annual 'Safer Internet Day, with specific teaching and discussion of eSafety issues. Other issues such as Cyber-bullying and 'Grooming' are discussed in PSHE sessions. All classes begin each academic year with a session reminding them of the 'Golden Rules for Staying Safe Online' and Acceptable Use Policy. Where necessary, class teachers will differentiate their teaching to ensure all pupils remain safe when using technology.
Pupils are also reminded of relevant legislation regarding the Internet, such as copyright implications. Pupils are taught during research lessons to critically evaluate materials and content. This is reinforced in all other cross-curricular ICT sessions.
The 'Golden Rules for Staying Safe Online' are displayed around school where a computer used.

6.2eSafety – Raising staff awareness

During the Autumn Term 2014, all staff will be required to attend INSET for an eSafety update (1st October). This will be led by a Lancashire Advisor. After which, they will all be required to sign the updated AUP. Any further updates will be led by Nicola Worth after she has completed the eSafety Champion Training.

All staff, upon starting work at the school, are required to agree to the school's AUP and are provided with a copy of the eSafety policy and key staff guidelines, which includes personal safeguarding. Staff training updates for eSafety will be delivered as necessary, with a minimum of once per academic year.

All staff are expected to promote and model responsible use of ICT at all times, and all staff are responsible for promoting eSafety whilst using ICT.

6.3eSafety – 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).

At Duke Street we hold an annual Parents eSafety Awareness meeting which is open to all parents. In autumn 2014, this will be presented by a Lancashire Advisor. After which it will be presented by Nicola Worth. This is advertised on the newsletters with an open invitation.

We have links to appropriate advice websites on our school website.

We also put reminders on school newsletter particularly during the Spring Term around the time on Internet Safety Day.

6.4 eSafety – Raising Governors' Awareness

At Duke Street we believe it is important that Governors, particularly those with specific curriculum and child protection responsibilities, are kept up to date. Governors are invited to parents and staff awareness sessions in school. They can also request meetings with the school's eSafety Champion for updates and to look at the incident book.

Governors who have access to computers within school are required to agree and sign the appropriate AUP.

The policy is approved and reviewed by the governors at least every 2 years.

7 Standards and inspection

Since September 2009 there has been greater emphasis on monitoring safeguarding procedures throughout schools.

The eSafety policy will be reviewed annually and will incorporate new technologies.

- A risk assessment will be carried out before any new technology is incorporated into teaching and learning. These risk assessments will be incorporated into the policy.
- eSafety incidents will be monitored and recorded by the eSafety Champion or Headteacher. These will be analysed to see if there is a recurring pattern.
- Patterns of eSafety issues will be addressed thorough assemblies, workshops and 'Circle Time' activities where appropriate.
- Changes to the eSafety policy will be discussed at staff meetings and staff will disseminate this information to pupils in an age-appropriate way.
- The eSafety policy will be reviewed by the curriculum sub-committee of the governing body and will be made available to parents.
- AUPs will be reviewed annually in the light of emerging technologies.

Appendices

Appendix 1 - Image Consent Form

Appendix 2 - ICT Acceptable Use Policy (AUP) – Staff and Governors

Appendix 3 - ICT Acceptable Use Policy (AUP) – Students, Supply Teachers, Visitors, Guests etc.

Appendix 4 - ICT Acceptable Use Policy (AUP) -Children FS / KS1

Appendix 5 - ICT Acceptable Use Policy (AUP) -Children KS2

Appendix 6 - eSafety Incident Log

Appendix 7 -Lancashire eSafety Incident/Escalation Procedures

Appendix 8 – Golden Rules to Staying Safe Online (EYFS/KS1)

Appendix 9 - Golden Rules to Staying Safe Online (KS2)

APPENDIX 1 – 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 1-6 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 use your child's image on our Facebook page? Yes / No
4. May we record your child on video? Yes / No
5. May we allow your child to appear in the media as part of school's involvement in an event? Yes / No
6. Will you allow us to use photos in which your child may appear, for use in school and the school website / Facebook page held in our archives? (this includes retaining photos for our archives after your child has left the school) Yes / No

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

Parent/Carer's signature:____

Name (PRINT):____

Date: ____

P.T.O

Conditions of Use

1. This form is valid for the your child whilst they are a pupil at Duke Street

2. The school will not re-use any photographs or videos after your child leaves this school without further consent being sought.

3. The school will not use the personal contact details or full names (which means first name **and** surname) of any pupil or adult in a photographic image, or video, on our website or in any of our printed publications.

4. If we use photographs of individual pupils, we will not use the full name of that pupil in any accompanying text or caption.

5. If we use the full name of a pupil in the text, we will not use a photograph of that pupil to accompany the article.

6. We will only use images of pupils who are suitably dressed.

7. 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

ICT Acceptable Use Policy (AUP) – Staff and Governors

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with 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, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with children and other adults are appropriate.
8. I will not use the school system(s) for personal use during working hours.
9. I will not install any hardware or software without the prior permission of *Mrs Worth*
10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
12. I will abide by the school’s rules for using personal mobile equipment, including my mobile phone, at all times.
13. I will report any known misuses of technology, including the unacceptable behaviours of others.
14. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
15. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
16. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
17. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
18. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.

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

User Signature

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

Signature ....

Date ....

Full Name ....(PRINT)

Position/Role ....

Appendix 3

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

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

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

User Signature

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

Signature ....

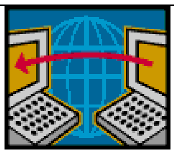
Date...

Full Name ....(PRINT)

Position/Role ....

Appendix 4 ICT Acceptable Use Policy (AUP) -Children FS / KS1

These rules reflect 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.

Think before you click	
S	I will only use the Internet when there is an adult in the room.
A	I will only click on icons and links that my teacher tells me or shows me.
F 	I will only send friendly and polite messages.
E	If I see something I don't like on a screen, I will always switch the monitor off and tell an adult.

My Name: ________________________________

My Signature: _____________________________

Parent / Carers Signature : ___________________

Appendix 5

ICT Acceptable Use Policy (AUP) -Children KS2

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

Signed .... **(Child)**

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 *Duke Street Primary School*
Parent /Carer Name (Print)..

Parent /Carer (Signature) ....

Class .... Date ....

Appendix 6 eSafety Incident Log

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

Date / Time of incident	Type of incident	Name of pupil/s and staff involved	System details	Incident details	Resulting actions taken and by whom (and signed)
28 Apr 2012 9.13 am	Accessing inappropriate website	A N Other (pupil) A N Staff (Class Teacher)	ICT suite computer 3	Pupil observed by CT to deliberately attempt to access adult websites	Pupil referred to HT and given 1st warning for unacceptable use. Parents informed via phone call from HT.

Appendix 7 Lancashire eSafety Incident/Escalation Procedures

**NB This appendices is available only in paper copy and is taken from the Lancashire ICT eSafety Guidance Document

Appendix 8

Classroom eSafety Rules (EYFS/KS1)

Our Golden Rules for Staying Safe Online

We only use the Internet when a grown up is with us.

We are always polite and friendly when using online tools.

We will only play games or look at websites that our teacher has shown us.

We always ask a grown up if we need help using the Internet.

We always tell a grown up if we find something that upsets us.

We will turn off the monitor and tell a grown up if we see something that upsets us.

A grown up is someone that you trust.

- Parents
- Grandparents
- Family

These Golden Rules have written by the School Council (September 2014)

Appendix 9

Classroom eSafety Rules - (KS2)

Our Golden Rules for Staying Safe Online

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 will only chat online with people a trusted adult has approved.

All our online chats 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 programmes which have been shown to us by the teacher.

BE SMART!

These Golden Rules have written by the School Council (September 2014)