Policy:	Online Safety
Reviewed:	November 2017
Next Review:	November 2018
Responsibility:	Headteacher/Governors
Category:	Safeguarding

Nelson St Philip's Church of England Primary School

Policy for Online Safety

Mission Statement

*We love to learn. We learn to love. With Christ as our Guide we love and learn together". **G**uide our children to prepare them for life; **R**espect themselves and one another; **A**spire to achieve their highest potential; **C**are for the local and wider community; **E**very child is special in God's eyes.*

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 Online safety Policy will help children develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our Online safety 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. The policy is organised in 4 main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection

Our school's vision for Online Safety

Our school strives to provide a diverse, balanced and relevant approach to the use of Technology, where children are encouraged to maximise the benefits and opportunities that technology has to offer.

Our school endeavours to ensure that children learn in an environment where security measures are balanced appropriately with the need to learn effectively.

Our children are equipped with the skills and knowledge to use technology appropriately and responsibly.

Our school teaches children how to recognise the risks associated with technology and how to deal with them, both within and outside the school environment.

All our school community understands why there is a need for an Online Safety Policy.

The role of the school's Online Safety Champion
Our Online Safety Champion is Mrs Shelley Swire

The role of the Online Safety Champion in our school includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school's Online Safety Policy and associated documents, including Acceptable Use Policies.
- Regular monitoring of all ICT users and their electronic history, in conjunction with the ICT Technician
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored
- Ensuring that all staff are aware of reporting procedures and requirements should an Online Safety incident occur.
- Ensuring that the Online Safety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up to date with Online Safety issues and guidance through liaison with the LA Schools' ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging Online Safety advice /training for staff, parents/carers and governors

Our school has used the following two documents to complete our Online Safety Policy

- The Lancashire Online Safety Framework Document (this document)
- The Lancashire Online Safety Guidance Document (used as a prompt for discussion)

Our completed Online Safety Policy forms part of the Lancashire Online Safety Charter.
For further information about the Lancashire Online Safety Charter please see http://www.lancsngfl.ac.uk/OnlineSafety

Developing and Reviewing this Policy

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

- Headteacher and Online Safety champion
- Staff
- Governors (including parents)
- Pupils

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

Policy Approved - Date: November 2017
Reviewed and approved: October 2017 Staff and November 22nd 2017 Govs

The implementation of this policy will be monitored by Headteacher and Online Safety Champion
This policy will be reviewed as appropriate by Headteacher and Governors annually

Approved by KD Ellidge (Headteacher) Date November 2017

Reviewed and Approved by KD Ellidge (Headteacher) Date October 2017

1. Policies and practices

1.1 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 this Online Safety Policy and statements in the Acceptable Use Policy (AUP).

The responsible person for management of information held is the Headteacher Mrs K Ellidge.

- Key personnel know the location of our data, as appropriate.
- All staff understand their legal responsibilities
- Notices of procedures are displayed in the Staffroom.
- Staff use only approved means to access, store and dispose of confidential data.
- Loss of data is minimised by limiting access to key personnel only and through encryption and password protection.

This Online Safety policy should be read in conjunction with the following other related policies and documents:

- Anti-bullying Policy (including Cyber Bullying)
- ICT Policy
- Induction Policy
- Visitors Policy
- Child Protection Policy (including information regarding PREVENT)

1.2 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 staff are aware that some mobile devices e.g. mobile phones, game consoles or net books can access unfiltered internet content
- All devices are virus checked before use on school systems.
- Pupils are not allowed to bring mobile phones into school in any circumstance. If mobile phones are brought into school by a pupil they will be kept in the School Office until the end of the school day and then passed to Parent/carer.

1.3 Use of digital media

In our school we are aware of the issues surrounding the use of digital media online. Access to the school's ICT Network will only be allowed to authorised persons. These persons will have limited access in accordance with responsibilities and can only access the network through personal ID Logins and passwords. All members of our school understand these issues and need to follow the school's guidance below.

1.4 Communication technologies

Email:

All digital communications will be professional in tone and content.

In our school the following statements outline our safe practice in our use of emails and how security is maintained.

- All users have access to the (Lancsngfl.ac.uk) Microsoft Online as the preferred school e-mail system.
- Only official email addresses should be used to contact staff/pupils.
- The Lancashire Grid for Learning filtering service should reduce the amount of SPAM
- (Junk Mail) received on school email accounts. Any incidents of SPAM will be
- reported to the BT One Connect.
- 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.
- Our school system incorporates a standard disclaimer at the bottom of all outgoing emails (see example below).

Example school e-mail disclaimer:
This e-mail and any files transmitted within it may be confidential and are intended solely for the individual to whom it is addressed. Any views or opinions presented are those of the author and do not necessarily represent St Aidan's C.E. School. If you are not the intended recipient, you must not use, disseminate, forward, print or copy this e-mail or its contents. If you have received this e-mail in error, please contact the sender. Please note that e-mail may be monitored in accordance with both school policy and the Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000.

Social Networks:

Many adults and pupils regularly use Social Network sites, e.g. Club Penguin, Moshi Monsters, Facebook or Twitter, although the minimum age for registering for some of these excludes primary school pupils. 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:

All staff need to be aware of the following points:

- They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
- Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- If a Social Network site is used, details must not be shared with pupils and privacy settings be set at maximum.
- Pupils must never be added as 'friends' on any Social Network site.
- Ensure all communications are transparent and open to scrutiny.
- All staff are aware that comments about the workplace or individuals therein are unacceptable

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. Ask yourself – Would you want your parents, children or your boss to see this now or in ten years time?

Mobile telephone:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Mobile telephones:

- Mobile telephones can be used in school by staff and visitors in designated areas only – the Staffroom and the PPA Room. They should not be used within the classroom.
- Mobile Telephones must only be used at **non-teaching times**, or **break times**, or in exceptional circumstances by specific prior arrangement with the Headteacher or Assistant Head.
- Staff mobiles must be kept securely in own possession – school will not be responsible for the loss or damage to this personal equipment
- Notices will be displayed in staffroom as to the accepted use of mobile telephones.
- No images of staff or pupils in school will be taken on mobile telephones, unless with prior permission.
- Mobile Telephones will not be used to support a lesson.
- Pupils will only be allowed a mobile telephone in school in exceptional circumstances and by prior arrangement with the Headteacher or Assistant Head. (This would be kept securely in the School Office).

Instant Messaging:

This is a popular tool used by adults and pupils that allows 'real time' communication and often integrates the ability to transmit images via a webcam. These sites are 'blocked' for use in Lancashire schools by default.

In our school the following statements outline what we consider to be acceptable and unacceptable use of Instant Messaging:

- Staff and children are made aware of the risks involved in this type of technology

Web sites and other online publications

Our school website is a vital means of communication with parents and pupils, and is protected by the company Web Anywhere, who monitors content and information available on the site.

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

- All online safety guidance is available on our school website
- Our website will not be used to share personal information.
- All school users are aware of guidance for the use of the website through our signed Acceptable User Policy Statements.

Video conferencing:

Our policy shows consideration of the etiquette, acceptable and unacceptable behaviour related to the use of VC in the classroom.

In our school the following statements outline what we consider to be acceptable and unacceptable use of Video conferencing:

- All communication should be in-line with our signed Acceptable User Policy Statements
- Parental permission will be accessed before video conferencing and/or photographs will be used, children appear 'live' on an internet link will be prior arrangement with the Headteacher.
- Approval from the Headteacher MUST be sought before any video conferencing takes place. All such sessions will be logged including date, time, and name of persons/organisation taking place.
- Pupils will be supervised by an adult at all times.
- Staff involved will be confident in the use of all procedures before commencing a video conference session.
- Copyright permission will be sourced before using any recorded images, sound or videos.

Others:

Use of other technologies i.e. Bluetooth systems or Infrared communication, at this time is NOT acceptable unless authorised by Headteacher or ICT Subject Leader.

1.5 Acceptable Use Policy (AUP)

Our Acceptable Use Policy ensures that all users of technology within school will be responsible and stay safe. This will ensure that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes. AUPs are used for Staff, Pupils and Visitors/Guests and must be signed and adhered to by users before access to technology is allowed. We consider our pupil AUPs as a partnership between parents/carers, pupils and the school to ensure that users are kept safe when using technology.

NB**A list of children who, for whatever reason, are not allowed to access technology will be kept in school and made available to all staff.

Our school has adopted the exemplar AUPs which are provided LCC E -Safety Guidance.

Our school AUPS must:

- Be understood by the each individual user and relevant to their setting and purpose.
- Be regularly reviewed and updated.
- Be regularly communicated to all users, particularly when changes are made to the
- Online Safety Policy/AUP.
- Outline acceptable and unacceptable behaviour when using technologies, for example:
- Cyberbullying
- Inappropriate use of email, communication technologies and Social Network
- sites and any online content
- Acceptable behaviour when using school equipment /accessing the school network.
- Outline the ways in which users are protected when using technologies e.g. passwords, virus protection and filtering.
- Provide advice for users on how to report any failings in technical safeguards.
- Clearly define how monitoring of network activity and online communications will take
- place and how this will be enforced.
- Outline sanctions for unacceptable use and make all users aware of the sanction.
- Stress the importance of Online Safety education and its practical implementation.
- Highlight the importance of parents/carers reading and discussing the content of the AUP with their child.
- Our school actively seeks opportunities to provide parents/carers with Online Safety updates and awareness meetings through Newsletters, the school website and offering a workshop each term.

1.6 Dealing with incidents

Here are the types of incident that may occur and how these will be dealt with in our school.
An incident log (see Appendix 11) will need to be completed to record and monitor offences. This will be audited on a regular basis by the online safety Champion or other designated member of the Senior Leadership Team.

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, LCC Safeguarding,CEOP, Internet Watch Foundation (IWF), PREVENT . **No staff member will ever personally investigate, interfere with or share evidence as they may inadvertently be committing an illegal offence.** It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident- (See Appendix 12).

Always report potential illegal content to the Internet Watch Foundation
(http://www.iwf.org.uk) .They are licensed to investigate – schools are not!

Examples of illegal offences are:
Accessing child sexual abuse images
Accessing non-photographic child sexual abuse images
Accessing criminally obscene adult content

Incitement to racial hatred

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

Inappropriate use

It is more likely that 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. Examples of inappropriate incidents are listed below with suggested sanctions for our school.

Incident	**Procedures 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 online safety Champion. Enter the details in the Incident Log. Additional awareness raising of online safety issues and the AUP with individual child/class. More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. Consider parent/carer involvement, for specific or repeated non-accidental incidents...
Deliberate searching for inappropriate materials.	
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate	

Procedures when dealing with Online safety;

- Responsible persons – Headteacher, Online safety Champion.
- All staff made aware of our procedures to recognise and deal with Online safety incidents
- Appendix 11 – Responding to safety incidents will be displayed in Staffroom as guidance
- Children are given online safety guidance as part of curriculum each half term
- Incidents will be logged on Form Appendix 10 in file in the school office and monitored by Online safety Champion
- Review of policy/procedures in line with frequency and seriousness of incidents

2. Infrastructure and technology

Our school subscribes to BT One Connect, and internet content filtering is provided by default. It is important to note that the filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service.

Our school offers the following guidance regarding security

Pupil Access:

Children are always supervised when accessing school equipment and online materials, working with a trusted adult at all times.

Passwords:

- All users of the school network have a secure username and password.
- The administrator password for the school network available to the ICT E- Safety Champion and the ICT Technician and kept in a secure place e.g. school safe
- Staff and pupils reminded of the importance of keeping passwords secret as part of regular online safety up-dates
- Staff are aware passwords need to be changed every 60 days.

Software/hardware:

- Our school has legal ownership of all software
- We have an up to date record of appropriate licences for all software and the Online safety Champion is responsible for maintaining this, with the ICT Technician.
- ICT Subject Leader and ICT Technician regularly audit equipment and software.
- ICT Subject Leader and ICT Technician controls the software available on our school network

Managing the network and technical support:

- ICT Technical support is provided by BT One Connect
- The Headteacher/ICT Subject Leader liaises with the ICT Technician - Western Business Systems
- Our server, wireless systems and cabling securely located.
- All wireless devices have had their security enabled and are accessed through a secure password.

- The Headteacher/ICT Subject Leader and ICT Technician is responsible for managing the security of our school network
- We review the safety and security of our school network through half termly checks.
- School systems are kept up to date in terms of security by the ICT Technician.
- All staff and pupils have a username and password assigned by ICT technician.
- All staff and pupils are required to log-out of computers when not in use.
- Only designated users, such as ICT Subject Leader, ICT Technician, and ICT Support Staff member, are allowed to download files or install software.
- All mobile storage devices are password protected and used for business use only.
- All staff remote access of emails etc. is through the school's secure network system from Lancs NGFL (Microsoft One)
- Only staff members have removable storage devices unless by prior arrangement with the Headteacher or ICT Subject Leader.

Filtering and virus protection:

- **Our school filtering service is provided by BTOneConnect .**
- We have requested devolved control over the BT One Connect filtering service. (See Appendix 1) e.g. access to YouTube through light filtering password protected systems.

3 Education and Training

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

There are 3 main areas of Online Safety risk and these are taught as an integral part of our curriculum. The three main areas of Online Safety risk that our school is aware of are;

1. COMMERCE

Pupils need to be taught to identify potential risks when using commercial sites.
Examples of risk include;

- Advertising e.g. SPAM
- Privacy of information (data protection,
- identity fraud, scams, phishing)
- Invasive software e.g. Virus", Trojans,
- Spyware
- Premium Rate services.
- On-line gambling

2. CONTENT

Pupils need to be taught that not all content is appropriate or from a reliable source.

Examples of risk include;

- Illegal materials
- Inaccurate/bias materials
- Inappropriate materials
- Copyright and plagiarism
- User-generated content e.g. YouTube

3. CONTACT

Pupils need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.

Examples of risk include;

- Grooming
- Cyberbullying
- Contact Inappropriate emails/instant messaging/blogging
- Encouraging inappropriate contact
- Incitement to radicalisation

3.1 Online Safety across the curriculum

It is vital that pupils are taught how to take a responsible approach to their own Online Safety. Our school endeavours to provide suitable Online Safety education to all pupils in the following ways:

- We provide regular, planned Online Safety teaching within a range of curriculum areas
- We have an additional focus on Online Safety during the National Online Safety Awareness Week (February)

- E- Safety education is differentiated for pupils with special educational needs through adult support.
- Pupils in Upper KS2 are taught of the relevant legislation when using the Internet e.g. Data Protection Act (1998) and copyright implications, when using the Internet as a research tool.
- Pupils made aware of the impact of Cyberbullying through PSHE and Online safety Week. They are aware of how to seek help if they are affected by these issues.
- Pupils are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.
- Through careful discussion we endeavour to ensure that pupils develop an understanding of the importance of the Acceptable Use Policy for ICT both within and outside school.
- School highlights safe Internet use in a number of ways e.g. classroom displays, e safety rules displayed, worship, PSHE, school website, letters home to parents etc.

3.2 Online Safety – Raising staff awareness

On-going CPD for all staff and volunteers who work in school is vital in maintaining vigilance with regard to Online safety. Our school delivers:

- A planned programme of formal Online Safety training for all staff to ensure they are regularly updated on their responsibilities as outlined in your school policy.
- Advice/guidance or training to individuals as and when required will be delivered as part of their Induction programme by the Online safety Champion or other nominated person to ensure that they fully understand both the school's Online Safety Policy and Acceptable Use Policy.
- Members of staff delivering Online Safety training have received external Online safety training/updates from a county provider/CEOP.
- Our school's Online safety training ensure staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites.
- All staff are expected to promote and model responsible use of ICT and digital resources.
- Regular safety up-dates are communicated to staff through Staff Meetings and by email.

3.3 Online Safety – Raising parents/carers awareness

Our school offers regular opportunities for parents/carers and the wider community to be informed about Online Safety, including the benefits and risks of using various technologies.

This is communicated in a number of ways;

- School newsletters.
- School Website.
- Bespoke Parents Online Safety Awareness sessions (one per term).
- New Reception Parents Induction
- Promotion of external Online Safety resources/online materials.

3.4 Online Safety – Raising Governors' awareness

All Governors, particularly those with specific responsibilities for Online Safety, ICT or child protection, are kept up to date through the following ways;

- discussion at Governor meetings,
- attendance at Local Authority Training, or CEOP
- Attendance at internal staff training – INSET
- Attendance at parent meetings.

The Online Safety Policy will be annually reviewed and approved by the governing body.

Written and approved 2015
Reviewed 2016
Reviewed 2017
November 2017

4 Standards and inspection

This monitoring of this policy is the responsibility of the Curriculum Committee of the Governing Body.

This policy will be monitored and reviewed by the following means;

- Pupil Attitude Questionnaires
- Termly reporting to Governors on Online Safety incidents, any patterns, and outcomes
- Termly report to Governors on Online Safety technology up-dates
- Governors review and adopt changes to policy, procedures, AUPs as appropriate

List of Appendices

Appendix 1..... Change request for devolved filtering control – my LGfL Filtering Interface

Appendix 2 ..... Example of Image Consent Form

Appendix 3 ..... Example of ICT Acceptable Use Policy (AUP) – Staff and Governors

Appendix 4 ..... Example of ICT Acceptable Use Policy (AUP) – Supply Teachers, Visitors/Guests

Appendix 5 ..... Example of ICT Acceptable Use Policy (AUP) – Pupils

Appendix 6 ..... Example of ICT Acceptable Use Policy (AUP) – Parent's letter

Appendix 7..... Example of Online Safety Rules (EYFS/KS1)

Appendix 8..... Example of Online Safety Rules (KS2)

Appendix 9..... Example letter – Parental Online Safety Awareness Session

Appendix 11..... 2013 Incident Log

Appendix 12..... 2013 Online Safety Incident/Escalation Procedures

APPENDIX 1 - Change Request for Devolved Filtering Control – my LGfL Filtering Interface

I would like to request devolved filtering control for my school through the my LGfL Filtering Interface. I understand that (with the exception of the mandatory 'Core Categories') this will allow the school to make local changes to the default filtering policies. Unless this is carefully managed, pupils and staff may have access to inappropriate content and materials and I accept that this would be the responsibility of the school.

I fully understand the implications this has relating to the wider Online Safety provision in school including the potential for misuse and can confirm that the school has the appropriate risk management policies and procedures in place to ensure this is managed accordingly (1).

Headteacher Name (print): ……

Headteacher LGfL email*: ……

Headteacher Signature: ……

Date: ……

School Name: ……

School District/Number: ……

* required for access to the LGfL filtering interface (e.g. head@exampleschool.lancs.sch.uk).
Note: Colleagues using non-LGfL email addresses (e.g. hotmail, yahoo, .com etc) will be contacted directly with setup details.
On **completion by the Headteacher**, please email the signed copy to 01257 516365.
Changes will be actioned as soon as possible but, dependent on demand, may take up to 2 working days to take effect.
1 **Important Note**: It is inappropriate for unfiltered Internet access to be made available within school settings. Schools opting to take local control of their filtering policy should be aware of the wider implications of unblocking certain categories and sites and how they will maintain their statutory obligations under the safeguarding agenda (e.g. Social Networking – Cyberbullying, Media Sharing - Inappropriate content). We would therefore strongly advise that any delegation of filtering control is carefully considered and limited to only a small number of appropriate staff who are explicitly aware of the school's policies and procedures. It is advisable that the School Online Safety Policy should reflect how blocking access to inappropriate sites will be managed as part of the school's Online Safety escalation procedures.

APPENDIX 2 – 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 printed publications, on our school website, or in school displays.

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

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

(Please Circle)

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

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

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

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

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

Parent/Carer's signature:_____

Name (PRINT):_____
Date: _____

P.T.O

Conditions of Use

1. This form is valid for this academic year – 2016-17

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 3 - ICT Acceptable Use Policy (AUP) –
Staff, Student, Volunteer and Governor Agreement

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 Online Safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.

3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.

4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, pupils or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.

5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.

6. I will respect copyright and intellectual property rights.

7. I will ensure that all electronic communications with pupils and other adults are appropriate.

8. I will not use the school system(s) for personal use during working hours.

9. I will not install any hardware or software without the prior permission of S Swire/A Graham

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 pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.

12. I will report any known misuses of technology, including the unacceptable behaviours of others.

13. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.

14. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.

15. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other user' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

16. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.

17. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.

18. I will take responsibility for reading and upholding the standards laid out in the AUP.

19. I will support and promote the school's Online Safety policy and help pupils 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 4 - ICT Acceptable Use Policy (AUP) –

Supply Teachers and Visitors/Guests Agreement

Mobile telephone:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Mobile telephones:

- Mobile telephones can be used in school by staff and visitors in designated areas only – the Staffroom and the PPA Room. They must not be used within the classroom.
- Mobile Telephones must only be used at non-teaching times, or break times, or in exceptional circumstances by specific prior arrangement with the Headteacher or Assistant Head.
- Staff mobiles must be kept securely in own possession – school will not be responsible for the loss or damage to this personal equipment
- Notices will be displayed in staffroom as to the accepted use of mobile telephones.
- No images of staff or pupils in school will be taken on mobile telephones.
- Mobile Telephones **will not be** used to support a lesson.

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 staff are aware that some mobile devices e.g. mobile phones, game consoles or net books can access unfiltered internet content
- All devices are virus checked before use on school systems.
- Pupils are not allowed to bring mobile phones into school in any circumstance. If mobile phones are brought into school by a pupil they will be kept in the School Office until the end of the school day and then passed to Parent/carer.

For use by any adult working in the school for a short period of time.

1. I have read and understand the school's policy on the use of mobile phones and similar devices.
2. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
3. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
4. I will respect copyright and intellectual property rights.
5. I will ensure that Images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy, on school equipment and with written consent of the parent/carer or relevant adult.
6. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
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 & Position / Role

…… (PRINT)

ICT Acceptable Use Policy (AUP) –

Pupils Agreement / Online Safety Rules

These rules reflect the content of Nelson St Philip's CE Primary School's Online Safety Policy.
****NB Parents/carers MUST read and discuss all the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet**.

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

……

Parent/ Carer Signature

We have discussed this Acceptable Use Policy and
…….... [Print child's name] agrees to follow
the Online Safety rules and to support the safe use of ICT at Nelson St Philip's CE Primary School.

Parent /Carer Name (Print) ……

Parent /Carer (Signature) ……

Class …… Date……

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

APPENDIX 6 –
ICT Acceptable Use Policy (AUP) – Parent's Letter

NELSON ST PHILIP'S C.E. PRIMARY SCHOOL

Dear Parent/Carer,

The use of ICT including the Internet, e-mail, learning platforms and today's mobile technologies are an integral element of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all pupils to act safely and responsibly when using technology both within, and outside of, the school environment. This is particularly relevant when using Social Network Sites which are increasingly popular amongst both the adult population and young people. However, many sites do have age-restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of these age-restriction policies and therefore we actively discourage this in our school.

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

Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible.
Along with addressing Online Safety as part of your child's learning, we will also be holding Parental Online Safety Awareness Sessions during the school year and I would take this opportunity to strongly encourage your attendance wherever possible. Further information on these sessions will be communicated as soon as dates are confirmed.

In the meantime, if you would like to find out more about Online Safety for parents and carers, please visit the Lancsngfl Online Safety website http://www.lancsngfl.ac.uk/Online Safety

Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguards the pupils in school.

If you have any concerns or would like to discuss any aspect of the use of ICT in school, please contact *Mrs Swire or Mrs Ellidge*

Yours sincerely,

Mrs K Ellidge
Headteacher

Be Responsible Stay Safe on the Internet

- Only use the Internet when there is a teacher or other adult with you.
- Only use your **class login and password**.
- **Never** give out your address or phone number.
- **Never** meet anyone you meet on the internet.
- All e-mails should be polite, appropriate and sensible.
- If you see anything unpleasant or if you feel uncomfortable about anything, **tell a grown up**.

Be sensible and be safe on the internet!

Be Responsible Stay Safe on the Internet

These rules for sensible internet use will keep you safe.

Please *make sure you understand and keep to them.*

The use of the Internet at school is for educational purposes.

- Only use the Internet when there is a teacher or other adult present to supervise, or when you have permission.
- Only use your **own login and password**.
- **Never** give out your address, phone number or arrange to meet someone.
- All e-mails should be polite, appropriate and sensible.
- If you receive a rude or offensive message you must report it to a member of staff **immediately**.
- If you see anything offensive or if you feel uncomfortable about anything, report it to your teacher.
- Be aware that the school may check your computer files and monitor the Internet sites you visit.
- Make sure that a web source is reliable and accurate.

You and your parents have signed the school Internet agreement. We trust that you will

Be sensible and be safe on the internet!

APPENDIX 9 – Parental Online Safety Awareness Session

<Insert School's Letterhead>

This example letter has been used by schools when hosting a Parents Online Safety Awareness session run by a consultant from Lancashire Schools' ICT Team.

Dear Parent/Carer,

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

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

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

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

Date: Time:

The session will address the following areas with time for you to ask questions:
What are our children doing online and are they safe?
Do they know what to do if they come across something suspicious?
Are they accessing age-appropriate content?
How can I help my child stay safe online?

Yours sincerely,

<The Headteacher>

I / we will be attending the above Parental Online Safety Awareness Session

*Name(s):*_____

Parent / Carer of: _____ *Year Group* _____

APPENDIX 10 – Online Safety Incident Log

All Online Safety incidents must be recorded by the School Online Safety Champion or designated person. This incident log will be monitored and reviewed regularly by the Headteacher and Chair of Governors. Any incidents involving Cyberbullying should also be recorded on the Integrated Bullying and Racist Incident Record Form 2' available via the Lancashire Schools 'Portal.

**NB this appendices is available only in paper copy and is taken from the Lancashire ICT Online Safety Guidance Document (available on the school's website

APPENDIX 11 – Responding to Online Safety Incident/ Escalation Procedures

**NB this appendices is available only in paper copy and is taken from the Lancashire ICT Online Safety Guidance Document (available on the school's website)