JONES MEMORIAL
PRIMARY SCHOOL

E SAFETY POLICY

"Used well, digital technologies are powerful, worthwhile educational tools; technical safeguards can partly protect users, but education in safe, effective practices is a key goal for schools." DENI circular 2007/01

UPDATED: AUGUST 2017

REVIEWED: AUGUST 2019

TO BE REVIEWED 2021

Signature of Chairperson of Board of Governors:_____

Signature of Principal:_____ Date _____

Contents

Jones Primary School E Safety Policy

DENI circular 2007/01 states:

> *"Used well, digital technologies are powerful, worthwhile educational tools; technical safeguards can partly protect users, but education in safe, effective practices is a key goal for schools."*

Rationale

The Boards of Governors has a duty to:

- safeguard and promote the welfare of pupils; and

  (Article 17 of the Education and Libraries (Northern Ireland) Order 2003).

- determine the measures to be taken at a school to protect pupils from

  abuse (*Article 18 of the Education and Libraries (Northern Ireland) Order*

  2003).

The rapidly changing nature of the Internet and new technologies means that e-Safety is an ever growing and changing area of interest and concern. The school has a duty of care to enable pupils to use on-line systems safely. This policy highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. It covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

This policy is largely based on DENI Circular 2007/1 *'Acceptable Use of the Internet and Digital Technologies in Schools' and DENI Circular 2011/22 'e-Safety Guidance' and* should also be read in conjunction with the School's Safeguarding policies. It has taken into account the recommendations of the *360 Degree Safe e-Safety Self Review Tool*. The school is currently working towards the E-Safety Accreditation Mark which recognises the school's commitment to e-Safety.

Aims: What is e-Safety?

E-Safety (electronic safety) in the school context:

- is concerned with safeguarding children in the digital world, with an emphasis on learning to understand and use technologies in a positive way;
- is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online;
- is concerned with supporting pupils to develop safer online behaviours both in and out of school; and
- is concerned with helping pupils recognise unsafe situations and how to respond to risks

appropriately.

ICT is a compulsory cross-curricular element of the N Curriculum and the school must ensure acquisition and development by pupils of these skills. The Internet and digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The school provides pupils with opportunities to use the excellent resources, along with developing the skills necessary to access, analyse and evaluate them.

Introduction

This document sets out the policy and practices for the safe and effective use of the Internet and digital technologies in the Jones Memorial Primary School and is brought to the attention of all stakeholders.

We aim to develop mature systems of e-Safety awareness, so that users can easily adapt their behaviours and become responsible users of any new technologies. As new technologies are developed, the school will respond quickly to any potential e-Safety threats posed by their use.

The policy has been drawn up by the school's e-safety committee.

E safety Committee:

Mrs Sandra Isherwood (Principal)

Mrs Kyra McMullin (ICT Co-ordinator and Designated E-Safety Co-ordinator)

Mr Scott Fallis (Parents and E-safety Nominated Rep on Board of Governors)

Mrs Roberta Bailie (Deputy Designated Child Protection Teacher, Senior Leadership Team and VP)

The policy has been approved by the Board of Governors and is available to all parents via the school website and as a hard copy, if requested. The policy and its implementation will be reviewed bi-annually.

1. Internet Services

1.1 Connectivity and Filtering

The school internet access is filtered for all users.

1.2 C2K

Classroom 2000 (C2k) is responsible for the provision of an ICT managed service to all schools in Northern Ireland. It provides a safety service which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse.

The updated service in 2016-17 allows for Improved Websense filtering which gives the school more flexible control. Customised filtering is managed by Mrs McMullin (E-Safety Co-ordinator) who has received additional training for this responsibility and can further amend the local filtering policy to the needs and demands of the school. This enables the school to access more internet sites to enhance teaching and learning. However, there are a number of agreed locked down sites that can never be overridden by the local school policy.

Internet use is monitored. Access to the Internet via the C2k Education Network is fully auditable and reports are available to the school principal. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal devices are allowed, C2K filtering will be applied that is consistent with school practice.

Some of the safety services include:

- Providing all users with unique user names and passwords
- Tracking and recording all online activity using the unique user names and passwords
- Scanning all C2k email and attachments for inappropriate content and viruses
- Filters access to web sites

2. Code of Safe Practice

When using the Internet, email systems and digital technologies, all users must comply with relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. Staff and pupils are made aware that use of the school's ICT resources is a privilege which can be removed.

The school has

(a) a Pupil Code of Practice (Appendix 1); and

(b) a Staff Code of Safe Practice (Appendix 2)

containing e-Safety Rules which makes explicit to all users what is safe and acceptable and what is not.

The scope of the Code covers fixed and mobile Internet; school PCs, laptops, iPads and digital video equipment. It should be noted that the use of devices owned personally by staff and pupils but brought onto school premises (such as mobile phones, camera phones, PDAs) is subject to the same requirements as technology provided by the school.

Mrs McMullin, the ICT Co-ordinator and the Senior Management Team will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology.

2.1 Code of Safe Practice for Pupils

A parental/carer consent letter (Appendix 3), accompanied by the Code of Practice for pupils, is issued to parents/carers at the beginning of the new school year. This consent must be obtained before the pupil accesses the internet.

The following key measures have been adopted to ensure pupils do not access any inappropriate material:

- The school's e Safety Code of Practice for Use of the Internet and other digital technologies is made explicit to all pupils;
- E-Safety guidelines are displayed prominently throughout the school;
- Pupils and their parents/carers are asked to sign the Code of Conduct sheets;
- Pupils, using the Internet, will normally be working in highly-visible areas of the school;
- All online activity is for appropriate educational purposes and supervised, where possible;
- Pupils will, wherever possible, use sites pre-selected by the teacher and appropriate to age group;
- Pupils are educated in the safe and effective use of the Internet, through a number of selected websites, including Superclubs and CEOPS.

It should be accepted, that however rigorous these measures may be, they can never be 100% effective. Neither the school nor C2K can accept liability under such circumstances.

Use of mobile phones by pupils is not permitted on the school premises during school hours. (Appendix 8)

2.2 Pupil Sanctions

We believe it is important that the school has a culture under which users understand and accept the need for e-Safety regulations and adopt positive behaviours, rather than one in which attitudes are determined solely by sanctions. Incidents of technology misuse which arise will be dealt with in accordance with the school's Behaviour Policy.

Minor school related incidents (whether in school or out of school) will be dealt with by Mrs McMullin and the Senior Leadership Team. This may result in parents being informed and a temporary ban on Internet use. Incidents involving child protection issues will be dealt with in accordance with the school's Safe Guarding Child Protection Policy.

Users will understand their responsibilities to report e-safety incidents. They will know and understand that there are clear systems for reporting abuse and understand that the processes must be followed rigorously. Incident reports will be logged by Mrs Isherwood on SIMS for future auditing, monitoring, analysis and for identifying serious issues or patterns of incidents. This will allow the school to review and update e-Safety policy and practices.

Pupils are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately. Users have an understanding of how to report issues online, including to CEOP.

2.3 Code of Safe Practice for Staff

The Code of Safe Practice has been agreed with staff.

- Pupils accessing the Internet should on the whole be supervised by an adult at all times.
- Staff will make pupils aware of the rules for the safe and effective use of the Internet. These are displayed in classrooms and discussed with pupils.
- Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to Mrs McMullin or Mrs Isherwood.
- In the interests of system security, staff passwords should only be shared with the network manager, Mrs McMullin.
- Teachers are aware that the C2K system tracks all Internet use and records the sites visited. The system also logs emails and messages sent and received by individual users.
- Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these.
- Photographs of pupils should, where possible, be taken with school equipment and images stored on a centralised i-mac, accessible only to teaching staff or under supervision for pupil work.
- School systems may not be used for unauthorised commercial transactions.
- A Staff Safe Code of Conduct, which details sanctions, is signed by all staff.

3. Internet Safety Awareness

We believe that, alongside a written e-Safety Policy and Code of Practice, it is essential to educate all users in the safe and effective use of the Internet and other forms of digital communication, both inside school and outside school. We see education in appropriate, effective and safe use as an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils.

3.1 Internet Safety Awareness for Pupils

A planned e-safety education programme for Years 1-7 takes place through both discrete lessons and wider curriculum opportunitiesThe school takes part in an e-Safety day in February and a BEE SAFE day in May. Pupils are also encouraged to enter e-Safety competitions, make posters and charts. Information is delivered and reinforced through school posters (for example Appendices 4, 5 and 6), the school website and newsletters. Rules for the Acceptable Use of the Internet (which have been drawn up with the aid of pupils) are discussed with all pupils and are prominently displayed in classrooms. Pupils are made aware of copyright and plagiarism. Pupils are encouraged to validate the accuracy of information which they research.

Resources:

Child Exploitation and Online Protection (CEOP) resources: a useful teaching tool looking at Internet safety and incorporated into our PDMU and ICT programme.

Childnet International www.childnet.com has produced materials to support the teaching of e-Safety at Key Stage One and Two. They have materials for parents and staff .

Other pupil resources available:

Superclubs, 360 e Safety Tool, *Signposts to Safety, KidSMART, Know IT All for Schools, ThinkUKnow*

3.2 Internet Safety Awareness for Staff/ Professional Development

Teachers are the first line of defence in e-Safety; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported. E-Safety training is therefore an essential element of our staff induction and part of an on-going Continuous Professional Development programme. Through our e-Safety policy, the school can ensure that all reasonable actions are taken and measures put in place to protect all users.

E-Safety training is linked with Safeguarding Training. Training needs are informed through audits. The induction programme for new staff includes e-Safety. The ICT Co-ordinator keeps informed and updated on issues relating to Internet Safety. All teaching staff, classroom assistants and supervisory assistants are in turn made aware of the Department's policy and strategy on ICT use in teaching and learning and are updated in relation to relevant changes. Staff uphold copyright regulations and intellectual property rights.

The Child Exploitation and Online Protection Centre (CEOP) runs regular one-day courses for teachers in Northern Ireland. Mrs Isherwood has attended training. Teachers can download lesson plans, teaching activities and pupils' worksheets by registering with the *Thinkuknow website.*

3.3 Internet Awareness for Governors

Mrs Isherwood keeps governors updated on e-Safety and e-safety issues. The Board of Governors has appointed Mr Scott Fallis as their representative on the school e-Safety Committee.

3.4 Internet Safety Awareness for Parents/ Carers and the Community

The Code of Safe Practice for pupils and Acceptable Use Agreement is sent home at the start of each school year for discussion with their child and parental signature. This e-Safety Policy and E-Safety materials are available on the school website. Internet safety leaflets for parents and carers (for example, Appendix 7) are sent home annually in February. Parents/carers' attention is drawn to the school website and school newsletter where e-Safety messages are given. The school organises a biannual talk on Internet safety, usually delivered by the PSNI for parents and the community. Parents are informed of the school's complaints policy which is on the school website. Parents are informed on how to report issues to the school. Parents and the community may access the Online Compass. www.onlinecompass.org.uk

3.5 Community Use of School ICT Resources

The school's ICT facilities are used as a community resource under the Extended Schools programme. Users are issued with separate usernames and passwords by C2K. The community may bring their own iPads and use these within the school's filtered policy. They must also agree to the school's Use of the Internet policy before participating and only access pre-selected and appropriate websites under the guidance of a tutor.

4. Health and Safety

We have attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT resources, both in classrooms and the ICT suite, which has been designed in accordance with health and safety guidelines and where pupils are supervised at all times. Guidance is issued to pupils in relation to the safe use of computers, interactive whiteboard and projectors. Such guidance includes advice concerning correct posture, positioning of screens, ensuring pupils do not stare directly into the beam of a projector etc. We are mindful of certain medical conditions which may be affected by use of such equipment e.g. photosensitive epilepsy.

4.1 Risk Assessments

Life in the 21st century presents dangers including violence, racism and exploitation from which pupils need to be reasonably protected. The school, to the best of its knowledge, has considered all new technologies wisely to ensure that it is fully aware of and can mitigate against the potential risks involved with their use. In so doing, pupils are informed of what to do if they come across inappropriate material or situations online.

4.2 Use of Mobile Phones

Most mobile phones have internet connectivity. Please refer to the schools Mobile Phone and Digital Technologies Policy (Appendix 6) on the use of such. Pupils do not bring mobile phones to school.

4.3 Digital and Video Images

Parental permission is gained when publishing personal images on the website or other publications. All members of the school understand their rights and responsibilities in the taking, use, sharing, publication and distribution of images (and in particular the risks attached).

Wireless Networks

The Health Protection Agency has advised that there is no consistent evidence of health effects from radio frequency exposures below guideline levels and therefore no reason why schools and others should not use WiFi (Wireless Fidelity) equipment. Further information on WiFi equipment is available on The Health Protection Agency website.

4.4 Personal Data

The school ensures all staff know and understand their obligations under the Personal Protection Act and comply with these to ensure the safe keeping of personal data, minimising the risk of loss or misuse of personal data. Staff have enhanced password protection with at least one capital letter and one number.

4.5 Cloud Storage

Data and information is stored on the Cloud, meaning it can be securely accessed from any location removing the need to carry data and files on insecure data pens and portable devices.

4.6 Social Media

Care will be taken when making use of social media for teaching and learning. While social media technologies can offer much to schools and pupils, however each brings its own unique issues and concerns. Each social media technology that is to be utilised will be risk assessed in the context of each school situation.

4.7 Cyber Bullying

Staff are made aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. This form of bullying is considered within the schools overall Anti-Bullying policy and Pastoral Care Policy as well as the e-Safety Policy.

Cyber Bullying can take many different forms and guises including:

- Email – nasty or abusive emails which may include viruses or inappropriate content.
- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile.
- Online Gaming – abuse or harassment of someone using online multi-player gaming sites.
- Mobile Phones – examples can include abusive texts, video or photo messages. Sexting occurs in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.
- Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.
- Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator. Pupils will be reminded that cyber-bullying can constitute a criminal offence.

While there is no specific legislation for cyber-bullying, the following covers different elements of cyber-bullying behaviour:

Protection from Harassment (NI) Order 1997 http://www.legislation.gov.uk/nisi/1997/1180

Malicious Communications (NI) Order 1988 http://www.legislation.gov.uk/nisi/1988/1849

The Communications Act 2003 http://www.legislation.gov.uk/ukpga/2003/21

Pupils are encouraged to report incidents of cyber-bullying to their parents and the school. If appropriate, the PSNI may be informed to ensure the matter is properly addressed and behaviour ceases. The school will keep records of cyber-bullying incidents on SIMS to monitor the effectiveness of their preventative activities, and to review and ensure consistency in their investigations, support and sanctions.

5. School Website

The school website www.jonesmemorial.co.uk is used to celebrate pupils' work, promote the school and provide information. The website reflects the school's ethos. Information is accurate and well presented and personal security is not compromised. The principal edits the website.

The following rules apply:

- The point of contact on the website is the school address, school e-mail and telephone number.
- Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected carefully. Parents who prefer their child's photographs do not appear on the school website is respected.
- Pupils' full names will not be used in association with photographs.
- The Principal will take overall editorial responsibility and ensure content is accurate and appropriate.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

6. Social Media

Community networks, chatrooms, instant messenger systems, online journals, social networks and blogs, enable sharing of resources, ideas, pictures and video amongst users, the majority of which, usually causes no concern. Concern, in relation to inappropriate activities, tends to emanate from use outside school. C2k filters out social networking sites and blocks attempts to circumvent their filters leaving it relatively safe in the school environment.

Safe and responsible use of social media is vitally important. It is addressed through our Internet Safety Education Programmes. We make staff, pupils and parents aware of the risks associated with the use of social media and encourage responsible use outside school. Information and education is provided for parents on the school website, school newsletter and at parent and community internet safety meetings. Instances of pupil/staff cyber bullying will be regarded as serious offences and dealt with according to the school's discipline policy and child protection procedures.

7. Monitoring and Self Evaluation

The school's wider self-evaluation processes (such as for an incoming School Development Plan) address e-safety in the overall ICT and Safeguarding Child Protection Policy reviews. All key stakeholders are part of the self-evaluative review and participate in questionnaires and surveys. Pupils offer a voice through school council meetings. The 360 Degree Self-Evaluative Review has enabled the school to address areas of need in order to obtain the Accredited E-Safety Mark. Monitoring records of e-safety incidents are presented to the Governors. This policy will be reviewed and amended in light of evidence provided by monitoring, updated technologies or new DE Guidance.

This policy should be read alongside the following: Pastoral Care Policy, Positive Behaviour Policy, Safeguarding Child Protection Policy, Anti Bullying Policy, Health and Safety Policy and the ICT Policy.

Appendices

Appendix 1: ICT Code of Safe Practice for Pupils

E Safety Rules

- ✔ I will log onto the My *School* Learning Platform with my own user name and password.
- ✔ I will only use ICT, including the internet, e-mail, iPad, digital video, mobile technologies etc. for school purposes.
- ✔ I will only use my class e-mail address or my own school e-mail address when e-mailing.
- ✔ I will only open e-mail attachments from people I know, or who my teacher has approved.
- ✔ I will not tell other people my ICT 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 not give out my own details such as my name, phone number or home address. I will not arrange to meet someone through an online activity 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 know that my use of ICT can be checked and that my parent/ carer will be contacted if a member of school staff is concerned about my e-Safety.

Pupil's Full Name …….... (printed) Class: …….

Pupil's Signature …….……. Date …….

Appendix 2: ICT Code of Safe Practice for Staff

ICT (including data) and the related technologies such as e-mail, internet and mobile devices are an expected part of our daily working life in school. This code of practice is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to agree to this code of practice and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs K McMullin (e-Safety Coordinator) or Mrs S Isherwood (Principal).

- ✔ I will only use the school's email or personal email (if approved by Mrs McMullin)/ Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Board of Governors.
- ✔ I will comply with the ICT system security and not disclose passwords provided to me by the school or other related authorities.
- ✔ I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- ✔ I will not give out personal details e.g. mobile phone number and personal e-mail address, to pupils and to parents.
- ✔ I will use the approved C2k secure e-mail system for school business.
- ✔ I will ensure personal data is kept secure and used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal or Board of Governors. Such data must be encrypted.
- ✔ I will not install any hardware or software on the C2K system without the permission of Mrs McMullin.
- ✔ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory on the C2K system or on the iPads.
- ✔ Images of pupils and/or staff will only be taken, stored and used for professional purposes online with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Principal.
- ✔ I understand that my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to Mrs McMullin or Mrs Isherwood (managers).
- ✔ I will respect copyright and intellectual property rights.
- ✔ I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- ✔ I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of practice and to support the safe and secure use of ICT throughout the school

Staff Member:……..... Signature

…….…….. Date ……. Full Name

…….. (printed) Job Title . . . . . .

Appendix 3: Parental Agreement/Consent Letter

Dear Parent/ Carer

It is essential that pupils are aware of e-Safety and know how to stay safe when using Information and Communications technology (ICT). As part of Jones Memorial Primary School's ICT programme we offer pupils supervised access to a *filtered* Internet service provided by C2k (PCs and Laptops). Access to the Internet enables pupils to explore and make appropriate use of many websites that are of enormous educational benefit. They can also exchange messages with other Internet users throughout the world. However in spite of the tremendous learning potential, you should be advised that some material accessible, via the Internet, may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

In order to help minimise any risks, which might arise from Internet use, our Service providers C2k have installed filtering software which operate by blocking thousands of inappropriate websites and barring inappropriate items, terms and searches in both Internet and e-mail. To further enhance safety, pupils will only use the Internet for educational purposes, under the supervision of a member of staff.

The school's rules for safe Internet use accompany this letter. Please read and discuss these with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation, please contact Mrs McMullin.

✂

Parent/ Carer signature

We have discussed this and …….....(child's name) agrees to follow the e-Safety rules and to support the safe use of ICT at Jones Memorial Primary School.

Parent/ Carer Signature …….…….

Date ……

Appendix 4: Samples of Classroom Posters

Key Stage 1

Think then Click

These rules help us to stay safe on the Internet

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 with an adult.

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.

Key Stage 2

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we are not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don’t know.
- We do not open e-mails sent by anyone we don’t know.
- We do not use Internet chat rooms.

Principles for Internet Use (Children's Version)

Be SMART on Line

S	**Secret:** Never give out your address, telephone number, username or password when on-line.
M	**Meeting** someone or group you have contacted on-line is not allowed without the permission and supervision of your parent or teacher.
A	**Accepting** e-mails, opening sites or files requires the permission of your teacher, appointed adult or parent.
R	**Remember** no offensive language, text or pictures are to be displayed, sent, copied or received.
T	**Tell** your parent, teacher or trusted adult if someone or something makes you uncomfortable.

Smile and Stay Safe Poster

e be displayed throughout the school

and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Appendix 5: Internet Access: Additional Advice for Parents

1. A home computer with Internet access should be situated in a location where parents can monitor access to the Internet.
2. Parents should agree with their children suitable days/times for accessing the Internet.
3. Parents should discuss with their children the school rules for using the Internet and implement these at home. Parents and children should decide together when, how long and what constitutes appropriate use.
4. Parents should get to know the sites their children visit and talk to them about what they are learning.
5. Parents should consider using appropriate Internet filtering software for blocking access to unsavoury materials. Further information is available from Parents' Information Network (address below).
6. It is not recommended that any child under 16 should be given unmonitored access to newsgroups or chat facilities.
7. Parents should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school name or financial information such as credit card or bank details. In this way they can protect their children and themselves from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud.
8. Parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages and to tell them if they receive any such messages or images. If the message comes from an Internet service connection provided by the school they should immediately inform the school.

Further advice for parents is available from the following sources:

- http://www.thinkuknow.co.uk Thinkuknow - a mock cybercafé which uses online role-play to help children from 5 to 16+ explore a range of issues.
- http://www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf Aimed at parents and carers, there is a great deal of very clear information about chat rooms, social networking sites, email and much more.
- http://www.parentscentre.gov.uk/usingcomputersandtheinternet A very comprehensive site aimed at parents and carers. Includes many articles and external links to other helpful sites.
- http://www.bbc.co.uk/webwise Includes an 'Internet for Beginners' course and a tool for answering your internet related questions.
- http://www.kidsmart.org.uk/ Explains the SMART rules for safe internet use and lots more besides.
- http://www.ceop.gov.uk/ The government's Child Exploitation and Online Protection Centre (CEOP)
- http://www.parents.vodafone.com Vodafone's site is designed to help parents and carers develop an understanding of their child's internet use

Appendix 6: Use of Mobile Phones and other Electronic Devices

Rationale

The Board of Governors of the Jones Memorial Primary School wish to ensure that all pupils are safe and well cared for. All staff and pupils have a right to work, enjoy and learn in a secure and caring environment. They also have a responsibility to contribute to the protection and maintenance of such an environment. The use of increasingly sophisticated equipment and integrated cameras could present a number of problems, hence, the co-operation of parents and carers with this guidance is very much appreciated.

It is therefore school policy to prohibit the unauthorised use by pupils of mobile phones or other electronic devices while on our school premises, grounds or on trips or activities e.g. school swimming.

Guidance

The school will adhere to the following guidance:

- While we fully acknowledge a pupil's right to have a mobile phone or other electronic device, we discourage pupils from bringing them to school. They are valuable items and might be vulnerable to damage, loss or theft. There is also the potential for inappropriate behaviour and potential bullying which could be harmful to other pupils or staff. Many have built - in cameras which could lead to child protection and data protection issues with regard to inappropriate photographs or distribution of images. We have a duty to protect all members of our school community.

- In an emergency situation, and with the express approval of a senior member of the school staff, or where a written request has been received from the parent/carer, the device may be stored in the school office. It is the child's responsibility to ask for the device at the end of the school day. Should parents need to contact pupils, or vice versa, this should be done following the usual school procedures: via the school office (02866323420).

- Pupils may only take photographs on school devices as part of a supervised educational activity which has been authorised by a senior member of staff.

- The school accepts no liability for the loss or damage of any electronic device which is in the pupil's possession during the school day.

- If a pupil is found by a member of staff to be using a mobile phone/electronic equipment for any purpose, the device will be confiscated from the pupil. The pupil must arrange for their parents/guardians to collect confiscated equipment from the School Office during normal working hours.

- Inappropriate photographs or video footage with a mobile phone or other electronic device of other pupils or teachers will be regarded as a serious offence and disciplinary action will be taken.

This policy supports the school's Health and Safety and Safe Guarding Policies: Anti-bullying, Child Protection, Positive Behaviour and Internet Acceptable Use policies. It has been endorsed by the Board of Governors and will be monitored, reviewed and amended as required.

Approved by the Board of Governors Reviewed in Aug 2019