

# Portway Junior School

## Online Safety Policy

## Contents of Online Safety Policy:

1. Introduction
2. Context and background
3. Roles and Responsibilities
4. Technical and Hardware Guidance
5. Online Safety for pupils
  - Internet access at school
  - Using the Internet for learning
  - Teaching the safe use of the Internet
  - Using email with pupils
  - Chat and online discussions
  - Other online technologies – mobile phones etc
  - Cyber Bullying
  - Contact Details and Privacy
  - Deliberate misuse – procedures and sanctions
  - Complaints
  - Online Safety Class Rules KS2
6. Use of ICT by school staff
7. Staff Acceptable Use Agreement form
8. Data Protection policy
9. ICT Loans to staff – agreement form

# 1. Introduction

Our Online Safety Policy has been written by the school.

It has been discussed with staff, agreed by the senior management and approved by Governors. It will be reviewed annually.

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties: the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Created by: Karen Puszczynska

Last Revised: 20<sup>th</sup> January 2017

To be revised:

## 2. Context and Background

### **The technologies**

ICT in the 21<sup>st</sup> Century has an all-encompassing role within the lives of children and adults. New internet and online technologies are enhancing communication and the sharing of information.

Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet – World Wide Web
- e-mail
- Instant messaging (often using simple web cams) e.g. Instant Messenger)
- Web based voice and video calling (e.g. Skype)
- Online chat rooms

- Online discussion forums
- Social networking sites (e.g. Facebook)
- Blogs and Micro-blogs (e.g. Twitter)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Video broadcasting sites (e.g. You Tube)
- Music and video downloading (e.g. iTunes)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, messaging and internet access

Our whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities
- Online Safety teaching is embedded into the school curriculum and schemes of work

### 3. Roles and Responsibilities

Online Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school.

#### **Leadership team**

The SLT ensures that the Policy is implemented across the school via the usual school monitoring procedures

#### **Online Safety Co-ordinator**

Our school Online Safety Co-ordinators are Sophie Waller and Iain Bly. They are responsible for keeping up to date on all Online Safety issues and ensuring that staff are updated as necessary.

#### **Governors**

The School Governing body is responsible for overseeing and reviewing all school policies, including the Online Safety Policy.

#### **School Staff**

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school Online Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

Staff should ensure they are familiar with the school Online Safety policy, and ask for clarification where needed.

They should sign the Staff Acceptable Internet Use agreement annually  
Class teachers should ensure that pupils are aware of the Online Safety rules, introducing them at the beginning of each new school year.

### **Pupils**

Pupils are expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with Online Safety issues, both at home and school.

They are asked to agree to a set of guidelines and rules covering their responsibilities when using ICT at school

### **Parents**

Parents are given information about the school's Online Safety policy at the Admission interview. They are given copies of the pupil for information, and asked to support these rules with their children.

## **4. Technical and hardware guidance**

### **School Internet provision**

The school uses RM Internet provider

### **Content filter**

Our Internet Provider uses a sophisticated content filter to ensure that as far as possible, only appropriate content from the Internet finds its way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter.

- All pupils and staff have been issued with clear guidelines on what to do if this happens, and parent will be informed where necessary.
- Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document.

### **Downloading files and applications**

The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.

- Pupils are not allowed to download any material from the Internet unless directed to do so by an appropriate staff member.

### **Portable storage media**

- Staff are allowed to use their own portable media storage (USB Keys etc). This is to be encrypted. If use of such a device results in an anti-virus message they should remove the device and immediately report to the ICT Administrator.

### **Security and virus protection**

The school subscribes to Sophos Antivirus software. The software is monitored and updated regularly by the school technical support staff

- Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to the ICT Administrator

## **5. Online Safety for Pupils**

We believe it is our responsibility to prepare pupils for their lives in the modern world, and ICT is an integral part of that world. At our school we are committed to teaching pupils to use the ICT effectively and appropriately in all aspects of their education.

### **Internet access at school**

#### **Use of the Internet by pupils**

Internet access is carefully controlled by teachers according to the age and experience of the pupils, and the learning objectives being addressed. Pupils are always actively supervised by an adult when using the Internet, and computers with Internet access are carefully located so that screens can be seen at all times by all who pass by.

#### **Access for all pupils**

In line with our inclusion policies across the school, we want to ensure that all our pupils have access to the Internet, particularly where this will directly support their learning.

### **Using the Internet for learning**

The Internet is now an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and a source of digital learning materials.

Using the Internet for learning is now a part of the Computing Curriculum (Sept 2014) We teach all of our pupils how to find appropriate information on the Internet, and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is.

- Teachers carefully plan all Internet-based teaching to ensure that pupils are focused and using appropriate and relevant materials.
- Children are taught how to use search engines and how to evaluate Internet-based information as part of the ICT curriculum, and in other curriculum areas where necessary.
- They are taught how to recognise the difference between commercial and non-commercial web sites, and how to investigate the possible authors of web-based materials.
- They are taught how to carry out simple checks for bias and misinformation
- They are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.

## Teaching safe use of the Internet and ICT

We think it is crucial to teach pupils how to use the Internet safely, both at school and at home, and we use the Kidsmart safety code to support our teaching in this area:

Kidsmart has been developed by the Childnet charity, and is endorsed by the DfES <http://www.kidsmart.org.uk>

The main aspects of this approach include the following five SMART tips:

- Safe - Staying safe involves being careful and not giving out your name, address, mobile phone no., school name or password to people online...
- Meeting someone you meet in cyberspace can be dangerous. Only do so with your parents'/carers' permission and then when they are present...
- Accepting e-mails or opening files from people you don't really know or trust can get you into trouble - they may contain viruses or nasty messages...  
Remember someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging end the conversation...
- Tell your parent or carer if someone or something makes you feel uncomfortable or worried...

### **Suitable material**

We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

### **Non-Education materials**

We believe it is better to support children in finding their way around the Internet with guidance and positive role modeling rather than restrict Internet use to strict curriculum based research. As well as Internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information, in free time at out-of-school-hours provision, and at home. There is a selection of links to such resources available from on the school website, and in the shared pupil folders on the school network.

### **Unsuitable material**

Despite the best efforts of the LA and school staff, occasionally pupils may come across something on the Internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken. The action will include:

- Making a note of the website and any other websites linked to it.
- Informing the ICT Administrator
- Logging the incident – ICT Incident Log Book in the school office
- Discussion with the pupil about the incident, and how to avoid similar experiences in future

## **Using E-Mail at school**

E-Mail is a valuable and stimulating method of communication that plays an important role in many aspects of our lives today. We believe it is important that our pupils understand the role of e-mail, and how to use it appropriately and effectively.

- We teach the use of e-mail as part of our ICT curriculum, and use appropriate pupil email accounts where necessary
- Pupils are not allowed to access personal e-mail using school Internet facilities

## Chat, discussion and social networking sites

These forms of electronic communication are used more and more by pupils out of school, and can also contribute to learning across a range of curriculum areas.

Online chat rooms, discussion forums and social networking sites present a range of personal safety and privacy issues for young people, and there have been some serious cases highlighted in the media.

We use the resources, guidelines and materials offered by Kidsmart, as outlined above in the Safe use of the Internet section to teach children how to use chat rooms safely.

All commercial Instant Messaging and Social Networking sites are filtered as part of the LA Internet policy

Pupils may take part in discussion forums or post messages on bulletin boards that teachers have evaluated as part of specific lesson activities. Individual pupil names or identifying information will never be used.

## Internet-enabled mobile phones and handheld devices

More and more young people have access to sophisticated new internet-enabled devices such as SMART mobile phones, tablets and music players.

It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the Internet, and allow pictures and information to be remotely posted to a website or weblog.

Pupils will be taught the legal and moral implications of posting photos and personal information from mobile phones to public websites etc and how the data protection and privacy laws apply.

- Pupils are not allowed to have personal mobile phones or other similar devices on their person in school. Parents may request that such devices are kept at the School Office for pupils who may need them on their journey to and from school.

## Cyberbullying - Online bullying and harassment

Online bullying and harassment via Instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on pupils. Our school has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy. These include:

- No access to public chat-rooms, Instant Messaging services and bulletin boards.
- Pupils are taught how to use the Internet safely and responsibly, and are given access to guidance and support resources from a variety of sources.

We encourage pupils to discuss any concerns or worries they have about online bullying and harassment with staff, and have a range of materials available to support pupils and their families.

- Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school child protection procedures.

## Contact details and privacy

As specified elsewhere in this policy, pupil's personal details, identifying information, images or other sensitive details will never be used for any public Internet-based activity unless written permission has been obtained from a parent or legal guardian.

Pupils are taught that sharing this information with others can be dangerous – see Teaching the Safe Use of the Internet.

## School and pupil websites – pictures and pupil input

As part of the ICT and wider curriculum, pupils may be involved in evaluating and designing web pages and web-based resources.

Any work that is published on a public website and attributed to members of our school community will reflect our school, and will therefore be carefully checked for mistakes, inaccuracies and inappropriate content.

Pupils may design and create personal web pages. These pages will generally only be made available to other school users, or as part of a password protected network or learning platform.

Where pupil websites are published on the wider Internet, perhaps as part of a project with another school, organisation etc, then identifying information will be removed, and images restricted.

## Deliberate misuse of the Internet facilities

All pupils have discussed the rules for using the Internet safely and appropriately. These rules should displayed in each classroom and the ICT suite

Where a pupil is found to be using the Internet inappropriately, for example to download games, or search for unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous misuse.

Sanctions will include:

Unsuitable material (e.g. online games, celebrity pictures, music downloads, sport websites etc)

- Initial warning from class teacher
- Report to Headteacher
- Letter to parent/carer

### **Offensive material**

- Meeting with Parent/Carer to re-sign Internet use agreement
- Subsequent incidents will be treated very seriously by the Headteacher, and may result in exclusion and/or police involvement.

## **How will complaints regarding Online Safety be handled?**

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

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

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- All incidents will be recorded
- Interview/counselling by class teacher, Senior Management Team, Online Safety Coordinator and Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period,
- referral to LA / Police.

Our Online Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher.

## 9. Use of the Internet and ICT resources by

### school staff The Internet

Our school understands that the Internet is a valuable resource for school staff. It provides a wealth of resources, teaching materials and information that teachers can use across the curriculum. It allows staff to share resources with other schools, and to engage in debate and discussion.

We are committed to encouraging and supporting our school staff to make the best use of the Internet and all the opportunities it offers to enhance our teaching and support learning.

### Internet Availability

To enable staff to make full use of these important resources, the Internet is available in school to all staff for professional use. The school also provides an OPENHIVE user account that gives further access to specific resources, online tools and email, Including <https://derbyshire.inthehive.net/learning/sitePages/home.aspx>

### ICT Equipment and Resources

The school also offers staff access to appropriate ICT equipment and resources, including computers, laptops, tablets, interactive whiteboards, data projectors, digital cameras, video

camcorders, sound recorders, control and data logging equipment and a range of professional and curriculum software

## Professional use

Staff are expected to model appropriate ICT and Internet use at all times. This supports our commitment to encouraging safe and appropriate ICT and Internet use by our pupils both in school and at home.

Staff are also careful to consider inclusion and equalities issues when using ICT and the Internet, and to provide pupils with appropriate models to support the school Inclusion and Equal Opportunities policies.

Staff who need support or INSET in using ICT as part of their professional practice can ask for support from the ICT Co-ordinator.

## Personal use of the Internet and ICT resources

Some equipment (including laptops) is available for loan to staff, with permission from the ICTCO and Headteacher. The appropriate forms and agreements must be signed.

However, all staff must be aware of the school policy on using school Internet and ICT resources for personal use. These are outlined in the staff agreement form below.

## E-mail

We recognise that e-mail is a useful and efficient professional communication tool. To facilitate this, staff members will be given a school e-mail address and we ask staff to use it for all professional communication with colleagues, organisations, companies and other groups.

Staff are reminded that using this e-mail address means that they are representing the school, and all communications must reflect this.

E-mail accounts provided by the school may sometimes need to be accessed, although personal privacy will be respected.

## Online discussion groups, bulletin boards and forums, online chat and messaging

We realise that a growing number of educationalists and education groups use discussion groups, online chat forums and bulletin board to share good practice and disseminate information and resources.

The use of online discussion groups and bulletin boards relating to professional practice and continuing professional development is encouraged, although staff are reminded that they are representing the school, and appropriate professional standards should apply to all postings and messages.

## Social Networking

The school appreciates that many staff will use social networking sites and tools. The use of social networking tools and how it relates to the professional life of school staff is covered in Staff Professional Conduct expectations and agreements.

## Data Protection and Copyright

The school has data protection policy in place – please see separate documentation for more details.

Staff are aware of this policy, and how it relates to Internet and ICT use, in particular with regard to pupil data and photographs, and follow the guidelines as necessary.

Staff understand that there are complex copyright issues around many online resources and materials, and always give appropriate credit when using online materials or resources in teaching and learning materials. They also support pupils to do the same.

# Portway Junior School

## Online Safety Policy Staff Agreement Form

This document covers use of school digital technologies, networks etc both in school and out of school. Access

- I will obtain the appropriate log on details and passwords from the Office Manager.
- I will not reveal my password(s) to anyone other than the persons responsible for running and maintaining the system.
- If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access school ICT system or resources

### Appropriate Use

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will never view, upload, download or send any material which is likely to be unsuitable for children or material that could be considered offensive to colleagues. This applies to any material of a violent, dangerous or inappropriate sexual content.
- I will not download, use or upload any material which is copyright, does not have the appropriate licensing or that might compromise the network
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Online Safety coordinator or member of the SMT.

### Professional Conduct

- I will not engage in any online activity that may compromise my professional responsibilities
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role
- I will never include pupils or former pupils as part of a non-professional social network or group
- I will ensure that I represent the school in a professional and appropriate way when sending e-mail, contributing to online discussion or posting to public websites using school facilities
- I will not browse, download or send material that could be considered offensive to colleagues
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact

### Personal Use

- I understand that I may use Internet facilities for personal use at lunchtimes and break time, where computers are available and not being used for professional or educational purposes.
- I understand that I may access private e-mail accounts during the availability periods outlined above for personal use, but will not download any attachments, pictures or other material onto school computers, or onto the school network area.
- I understand that the forwarding of e-mail chain letters, inappropriate 'jokes' and similar material is forbidden.
- I will not use the school Internet facilities for personal access to public discussion groups or social networking sites

#### Email

- I will only use the approved, secure email system for any school business: (currently: Outlook 365 Mail)
- I will only use the approved school email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.

#### Use of School equipment out of school

- I agree and accept that any computer or laptop loaned to me by the school, is provided mainly to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue and Customs.
- I will return school equipment regularly (to be agreed with ICT Administrator) to be checked and updated
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software

#### Teaching and Learning

- I will always actively supervise, or arrange for suitable supervision of pupils that I have directed or allowed to use the Internet
- I will embed the school's Online Safety curriculum into my teaching, using agreed resources and materials
- I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice
- I will only use the Internet for professional purposes when pupils are present in an ICT suite, or a classroom with Internet access

#### Photographs and Video

- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission
- I will never associate pupil names or personal information with images or videos published in school publications or on the Internet (in accordance with school policy and parental guidance)

#### Data protection

- I will not give out or share personal addresses (including email), telephone / fax numbers of any adult or students working at the school.
- I will not take pupil data, photographs or video from the school premises without the full permission of the head teacher e.g. on a laptop, memory stick or any other removable media
- I will ensure that I follow school data security protocols when using any confidential data at any location other than school premises
- I will respect the privacy of other users' data, and will never enter the file areas of other staff without their express permission
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

### Copyright

- I will not publish or distribute work that is protected by copyright
- I will encourage pupils to reference online resources and websites when they use them in a report or publication

### User Signature

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Online Safety policies.

I agree to have a school user account, be connected to the Internet via the school network and be able to use the school's ICT resources and systems.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

School .....

Authorised Signature Head Teacher approve this user to be set-up.

Signature ..... Date .....

Full Name ..... (printed)

## 11. Data Protection Policy

Our school is aware of the data protection law as it affects our use of the Internet, both in administration and teaching and learning.

We adhere to the LA Guidelines on Data protection.

Staff and pupils understand the legal and disciplinary implications of using the Internet at school for illegal purposes.

Where appropriate, the police and other relevant authorities will be involved in cases of deliberate misuse or abuse of the Internet by members of the school community using the connection provided by the school.

## 12. Staff Laptop and ICT Equipment Loans

Any member of staff who borrows or uses a school laptop, computer or any other ICT equipment must adhere to all aspects of this Online Safety Policy.

This must be the case wherever the laptop, computer or other such device is being used as it remains the property of Portway Junior School at all times.

Staff must undertake to take proper care of the equipment whilst in their possession and will abide by the requirements of the school's insurance policy with regard to protecting the equipment from loss or damage. They must also agree that, should the equipment be lost or damaged due to exposure to a non-insured risk, they will replace or arrange for the repair of the equipment at their own expense.

Staff must sign the 'Staff Laptop and Computer Loans Agreement' before taking the equipment away from the school premises.

## Staff Laptop and ICT Equipment Loan Agreement

I have borrowed a school laptop to use out of school in agreement with both Head Teacher and the ICT coordinator.

Make:

Model:

Serial number:

It is understood that I will return the equipment to school if requested to do so by either the Head Teacher

I undertake to take proper care of the equipment whilst in my possession and will abide by the requirements of the school's insurance policy with regard to protecting the equipment from loss or damage. I agree that, should the equipment be lost or damaged due to exposure to a non-insured risk, I will replace or arrange for the repair of the equipment at my own expense.

I will use the equipment in accordance with the schools Online Safety Policy and Staff Acceptable Use policy.

I agree to the above conditions:

(Signature) \_\_\_\_\_

(Print name) \_\_\_\_\_ Date:

Returned: \_\_\_\_\_ Date:

## **Responsible Internet Use: Portway Junior School**

We use the school computers and Internet connection for learning. These rules will help us to be fair to others and keep everyone safe.

- I will ask permission before entering any Web site (including social networking sites), unless my teacher has already approved that site.
- On the network, I will use only my own class login and password, which I will keep secret.
- I will not look at or delete other people's files.
- I will not bring data storage devices such as USB memory sticks into school without permission and I will not use them until they have been virus-checked.
- I will only e-mail people my teacher has approved.
- The messages I send will be polite and sensible.
- When sending e-mail or using the internet, I will not give my home address or phone number, or arrange to meet someone.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I will not use any Internet chat room or discussion facility other than the school's learning portal.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I know that the school may check my computer files and may monitor the Internet sites I visit.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.

## **Portway Junior School**

Dear Parents

### **Responsible Internet Use**

As part of your child's curriculum and the development of ICT skills, our school is providing supervised access to the Internet. We believe that the use of the Web and e-mail is worthwhile and an essential tool for children as they grow up in the modern world. I enclose a copy of the rules for Responsible Internet Use that we operate at our school.

Although there have been concerns about pupils having access to undesirable materials at other schools, we are taking positive steps to deal with this risk at Portway Junior School. Our school Internet access provider operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable under any circumstances for any damages arising from your child's use of the Internet facilities.

**Please would you read the rules for Responsible Internet Use and sign and return the consent form so that your child may use the internet at school.**

Should you wish to discuss any aspect of Internet use please telephone me to arrange an appointment.

Yours sincerely

Mrs K Puszczynska  
Headteacher

**Portway Junior School**

**Responsible Internet Use**

Please complete, sign and return to your child's class teacher.

***Pupil:***

**Pupil Agreement**

I understand the school rules for responsible Internet use. I will use the computer system in a responsible way and obey these rules at all times.

***Signed:***

***Date:***

**Parent Consent**

I have read and understood the school rules for responsible Internet use and give permission for my son or daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

***Signed:***

***Date:***

***Please print name:***

**Parent's Consent for Web Publication of Work and Photographs**

I agree that, if selected, my son/daughter's work may be published on the school Web site. I also agree that photographs that include my son/daughter may be published subject to the school rules that photographs will not clearly identify individuals and that full names will not be used.

***Signed:***

***Date:***

**References**

## Particularly for Parents

### **National Action for Children (NCH)**

Parents Guide on Internet usage  
Current activities to promote safe use

**Internet Watch Foundation** - report inappropriate Web sites [www.iwf.org.uk](http://www.iwf.org.uk)  
Safe Surfing Guide for parents and carers: [www.iwf.org.uk/safe/](http://www.iwf.org.uk/safe/)  
Which article on Internet filtering for home use [www.iwf.org.uk/safe/which/total.htm](http://www.iwf.org.uk/safe/which/total.htm)

**Parents Information Network (PIN)** [www.pin.org.uk/learning/safeindx.htm](http://www.pin.org.uk/learning/safeindx.htm)  
Comprehensive guidelines on Internet safety

### **Recreational Software Advisory Council (RSACi)**

Promotes rating systems for Web sites, and is a third party rating bureau

## Particularly for Schools

### **Associations of Co-ordinators of IT (ACITT)**

<http://atschool.eduweb.co.uk/acitt/aup.html>

Acceptable use policy for the Internet in UK Schools

**BECTa** [www.becta.org.uk/technology/infosheets/html/accuse.html](http://www.becta.org.uk/technology/infosheets/html/accuse.html)  
Advice and guidance on appropriate computer use

### **British Computer Society**

[www.bcs.org.uk/iap.html](http://www.bcs.org.uk/iap.html)

A guide for schools prepared by the BCS Schools Committee  
and the National Association of Advisers for Computer Education (NAACE)

### **DfEE Superhighway Safety**

<http://safety.ngfl.gov.uk>

Essential reading. For free pack telephone: 0845 6022260

### **Internet Watch Foundation -**

[www.iwf.org.uk](http://www.iwf.org.uk)

Invites users to report illegal Web sites

### **SEGfL ICT Security Policy**

[www.segfl.org.uk/](http://www.segfl.org.uk/)

An overview of the security of networks with Internet access.

## Copyright

[www.templetons.com/brad/copymyths.html](http://www.templetons.com/brad/copymyths.html)

Covers the main aspects of copyright of digital materials, US-based but relevant.

### **Internet Users Guide**

[www.terena.nl/libr/gnrt/](http://www.terena.nl/libr/gnrt/)

A guide to network resource tools, a book (ISBN 0-201-61905-9) or free on the Web

## Portway Junior School

## School Laptop Loan Agreement

The Headteacher has agreed that a laptop computer will be loaned to you while you remain employed at this school. This loan is subject to review on a regular basis, and can be withdrawn at any time. As a member of staff to whom a laptop has been loaned I have read and agree to the following terms and conditions that apply while the laptop is in my possession:

1. The Laptop, and any accessories provided with it, remains the property of Portway Junior School and is strictly for my sole use to assist staff in the performance of their job. Laptops must not be used by anyone not employed by the school.
2. I understand insurance cover provides protection from the standard risks but excludes theft from a vehicle. If the laptop is stolen from an unattended vehicle or a house left unattended for longer than 48 hours, I will be responsible for its replacement.
3. I agree to: treat the laptop with due care and keep the laptop in good condition, ensure that it is strapped in to the carry case when transported and/or not in use, not leave the laptop unattended in class without being secured and avoid food and drink near the keyboard/touch pad.
4. I agree to back up my work on a regular basis. I understand the school will not accept responsibility for the loss of work in the event of the laptop malfunctioning.
5. I agree to only use software licensed by the school, authorised by the Headteacher and installed by the school's ICT staff.
6. I agree that Anti-Virus software is installed and must be updated on a weekly basis. ICT staff from the school will advise on the routines and schedule of this operation.
7. Should any faults occur, I agree to notify the school's ICT staff as soon as possible so that they may undertake any necessary repairs. Under no circumstances should I, or anyone other than ICT staff, attempt to fix suspected hardware, or any other faults.
8. I agree to attend training in how to access the Curriculum Network, Intranet, Internet, and email within the school provided by ICT staff.
9. I agree that home Internet access is permitted at the discretion of the headteacher. I understand the school will not accept responsibility for offering technical support relating to home Internet connectivity.
10. I agree that any telephone/broadband charges incurred by staff accessing the Internet from any site other than school premises are not chargeable to the school.
11. I agree to adhere to School and LA policies regarding the following, updated as necessary:
  - Acceptable use,
  - Data protection,
  - Computer misuse,
  - Health and safety.

### **Note on Insurance**

For laptops to be covered automatically under the schools policies at no extra charge, they need to be included on the school's inventory. The standard All Risks insurance policy covers the laptops for theft (where there are signs of forced entry), and accidental or malicious damage.

Laptops are not covered by the school policy:

- Whilst in vehicles,
- Left unattended in a locked household over 48 hours.

## **Staff Guidance on Staying safe with use of New Technologies**

### Acknowledgement

This document has been adapted for use within Portway Junior School from the original document 'Safer Practice with Technology for Adults working in schools' produced by Kent

Public Service Network

[www.kenttrustweb.org.uk/esafety](http://www.kenttrustweb.org.uk/esafety)

### Questions

#### **Q1 Can I use my mobile phone to take photographs or video of students?**

Photography by pupils and staff are encouraged for curriculum use and are an essential part of any school visit, but there are potential dangers. The safest approach is to avoid the use of personal equipment and to use a school-provided item. A potential danger is an allegation that an adult has taken an inappropriate photograph. With a personal camera it would be more difficult for the adult to show that this was not the case. With school equipment there is at least a demonstration that the photography was consistent with school policy. It is important that the Guidance on the Use of Photographic Images of Children is referred to [www.gowild.org.uk/dataprotection](http://www.gowild.org.uk/dataprotection) Care should also be taken that photographs are stored appropriately. For instance to copy the photograph on to a personal laptop as opposed to a school allocated laptop might make it difficult to retain control of how the picture is used.

Memory cards, memory sticks and CD's should only provide a temporary storage medium.

Once photographs are uploaded to the appropriate area of the school network images should be erased immediately from their initial storage location.

## **Q2 Should I continue to use my Social Networking site?**

Social networking is a 'normal' part of life for most young people and many adults. However, adults working with children and young people should review and reflect upon their use of social network sites as they take on professional responsibilities. This includes checking back on redundant sites that may still be active. Strong passwords should be used and security settings should be applied so that **you** control all access to your profile. Once Information is published, (photographs, blog posts etc.) you lose control of them and they may be manipulated without your consent, used out of context, inappropriately or distributed further. What might seem an amusing remark posted about your school or colleagues, may end up re-published elsewhere by "friends" False social networking sites have been set up by pupils and staff with malicious information. Currently few public social networking sites authenticate their members and use automated registration systems which provide limited if any checks. Some instant messaging applications such as MSN have a facility to keep a log of conversations. "Don't publish or say anything online that you would not write down and display on the staff room notice board.

## **Q3 Is it alright to have pupils/students/parents as friends on my social network site or instant messaging service?**

Communication between adults and children/young people, by whatever method, should take place within clear and explicit professional boundaries. Staff should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child / young person, other than that which might be appropriate as part of their professional role. Therefore, requests to be a 'friend' on any social network site should be ignored. "Adults should ensure that all communications are transparent and open to scrutiny." (DCSF Nov 2007) For example ensuring all communications by all parties, use official school email or Learning Platform systems and is purely for teaching and learning purposes. Consideration should be given as to how communications might appear to a third party. Compared with a conversation in school the use of new technology inevitably increases the potential for messages to be seen out of context or misinterpreted. Staff must use an online environment which is under the school's or Local Authority's control. The first requirement is that you know who you are talking to; users must be authenticated. A School/Local Authority/RBC provided communication and collaboration area will have a range of security features set within a policy framework.

## **Q4 What is my responsibility for the use of my school laptop at home?**

Access to wider sites by family members, for instance accessing gaming site or less well known shopping sites will increase the risk of virus attack, unwanted adware and identity theft. If another member of the family or a friend is allowed to use the computer it is difficult to ensure that the use has been appropriate, for instance that

confidential information has not been accessed. Adults' views vary enormously in their judgements as to what is appropriate! The use of a school laptop to view adult material outside school hours and at home is inappropriate and may be illegal. The schools acceptable use policy should clearly state what is acceptable. There are cases where inappropriate access has led to dismissal.

School staff need to remember that in order for anyone else to use a school laptop in the home setting, they would need to be logged on by the person responsible for the laptop.

Increasingly the use of a school computer for non-professional use is being explicitly banned by schools. School staff should therefore ensure that they have absolute control of a school laptop allocated to their use.

### **Q5 What is inappropriate material?**

Inappropriate is a term that can mean different things to different people. It is important to differentiate between 'inappropriate and illegal' and 'inappropriate but legal'. All staff should be aware that in the former case investigation may lead to criminal investigation, prosecution, dismissal and barring. In the latter it can still lead to disciplinary action, dismissal and barring even if there is no criminal prosecution.

**Illegal** Possessing or distributing indecent images of a person under 18 – viewing such images on-line may well constitute possession even if not saved. What is regarded as indecent would ultimately be down to a jury to decide. The police have a grading system for different types of indecent image. Remember that children may be harmed or coerced into posing for such images and are therefore victims of child sexual abuse.

**Hate/Harm/Harassment** There is a range of offences to do with inciting hatred on the basis of race, religion, sexual orientation etc. *Individual:* There are particular offences to do with harassing or threatening individuals – this includes bullying by mobile phone, social networking sites etc. (cyberbullying). It is an offence to send indecent, offensive or threatening messages with the purpose of causing the recipient distress or anxiety.

**Inappropriate** Think about this in respect of professionalism and being a role model. The scope here is enormous, but bear in mind that "actions outside of the workplace that could be so serious as to fundamentally breach the trust and confidence placed in the employee"

(SPS 2004) may constitute gross misconduct.

#### **Some possible examples:**

- Posting offensive or insulting comments about the school on Facebook.
- Accessing inappropriate material on school devices.
- Making derogatory comments about pupils or colleagues on social networking sites.
- Contacting pupils by personal email or social networking site.

### **Q6 How should I store personal data safely?**

Teachers often find it convenient to write pupil reports or staff appraisals and references at home. This may require access to confidential personal information. Family Services and eservices are working on providing practical guidance for schools in keeping data secure.

Guidance on Information security can be found at [www.gowild.org.uk/esafety](http://www.gowild.org.uk/esafety) All personal information must be kept secure. Making such storage secure may include password protection, encryption of data and locking the computer when not in use. Please refer to the guidance document on information security referred to above and your ICT support service.

The mislaying a memory sticks are all too common. Even the use of encrypted memory sticks should only be seen as temporary storage of personal data, and only if necessary and ensuring files are deleted after use. The safest long-term storage location may be the school network. "Information security is an integral part of the Data Protection Act 1998. You must take all reasonable steps to ensure that any personal information that all staff are strongly advised to ensure that they understand the school policy regarding data protection. All schools should have a data protection policy.

### **Q7 How can I use ICT appropriately to communicate with young people?**

Using ICT to communicate with pupils/young people should be done through the school's Learning Platform in an appropriate online open shared environment such as a class forum.

Friendly verbal banter between adult and pupil may not be inappropriate, but it might look very different if carried out via email and might lead to difficulties if misinterpreted, forwarded or used out of context. See Q3 On no account should staff use their personal email addresses, social networking sites or phone numbers/texts to communicate with young people unless they are directly related or unless sanctioned by the head teacher.

### **Q8 As a technician, how can I safely monitor school network use?**

If the school has monitoring software in place for recording network activity, this can only be effective if monitored carefully to notice and report inappropriate access or usage. This is a senior responsibility and will require oversight and allocated time of a senior member of staff.

Leaving this role solely to a technician in school is not adequate and the responsibility can become onerous if a pupil or staff member is apparently implicated in inappropriate or illegal activity. Careful consideration about the use of monitoring software should be given and all staff and pupils informed if applied to the network. Educating pupils/young people about appropriate online behaviour in school and outside school be an integral part of teaching and learning programmes. It is wrong to assume that filtering and monitoring are simply technical ICT activities, solely managed by the network staff. Some technical staff have indeed taken on this wider responsibility to help ensure that ICT use is appropriate and beneficial.

However technical staff should not be expected to make judgements as to what is inappropriate material or behaviour, without support and supervision. Monitoring policy must be set by the senior leadership team, with set procedures to deal with incidents. The senior leadership team will require assistance from technical staff, but must also involve the school designated child protection Leader and pastoral staff. A technician might, with the best of intent, check sites that a user has visited and email images to alert a colleague. Should the images prove to be illegal the technician has

committed a criminal offence. A defence may be that the technician was acting within a published school procedure, but staff should ensure that they receive a specific, written request to perform this work. Should an incident of concern occur, there should be a clear route for immediate reporting to a senior leader. Procedures to preserve evidence by unplugging a computer or locking an account need to be in place.

**If in doubt**

- Consult with your line manager and school policies.
- Consider how an action would look to a third party.
- Only publish content that you would be happy to share with parents, pupils and your employer.

**Laptop Details**

Laptop Make ..... Model. ....

Serial Number ..... School Code .....

**Personnel Details**

Loan Authorised by .....

Head teacher: ..... Date .....  
(signature)

I have read and agree to be bound by the terms and conditions set out above.

Name of Member of Staff .....

Received by (signature): ..... Date .....

Any theft should be immediately reported to the police and a crime reference number should be obtained and provided to Bursar. If stolen or damaged from an employee's home, the school would first ask for a claim under the staff member's household policy.

Claims from the School policy will only be made if this were unsuccessful. Please note that regardless of the policy a stolen laptop is claimed under, a claim will not be considered unless there are signs of forced entry or assault.

Reviewed School Development Sub - Committee

Date approved : February 2017

By :

- School Development Sub Committee

Date of next review : February 2018