

**Safe, Effective and Acceptable Use of the Internet**

**&**

**Digital Technologies/ Online Policy**



# St.Joseph’s Primary School

Chair of the Board of Governors – Mr Niall Addis

Policy reviewed and updated by staff —

Policy reviewed and ratified by Governors-

**Signature of Chair\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Policy Updated March 2018)

“Online safety means acting and staying safe when using digital technologies. It is wider than simply internet technology and includes electronic communication via text messages, social environments and apps, and using games consoles through any digital device. In all cases, in schools and elsewhere, it is a paramount concern.”

***DENI Safeguarding and Child Protection in Schools: A guide for Schools (May 2017)***

**Rationale**

The use of technology is now an integral part of children’s education and interaction. The statutory requirements for UICT (Using Information and Communication Technology) as a cross curricular skill states pupils need to explore (find and use information) and express (create and present ideas) within information technology, evaluate (review learning and process) exchange (work collaboratively online) and exhibit (showcase their work digitally).

By doing this we are developing children’s ICT skills needed for life: social interactions, future learning and computer literacy for all careers.

The Internet technologies children and young people are currently using, both inside and outside of the classroom, include:

• Websites

• Learning Platforms and Virtual Learning Environments

• Email and Instant Messaging

• Chat Rooms and Social Networking

• Blogs and Wikis

• Podcasting

• Video Broadcasting

• Music Downloading

• Gaming

• Mobile/Smart phones with text, video and/or web functionality

• Other mobile devices with web functionality

Staff at St Joseph’s integrate the use of the internet, email and digital technologies daily as a teaching / learning tool to raise standards and promote achievement. ICT is also used in the management of school information and for administration purposes.

This policy has been created in line with:

* DENI Circular 2016/27 “*Online Safety*”
* DENI Circular 2016/26 *“Effective Educational Uses of Mobile Digital Devices”*
* *360 Degree Online Safety Self-Review Tool for Schools* (May 2017) https://360safe.org.uk/Overview (Recommended by EA Belfast)
* DENI “*Safeguarding and Child Protection in Schools: A Guide for Schools”* (May 2017)

The policy is integrated into our Pastoral Care, Positive Behaviour Policy and Safeguarding and Child Protection Policy. It incorporates agreements on the acceptable use of (i) the internet and school-based digital technology and (ii) personal mobile technology.

This policy applies to all members of St. Joseph’s PS; pupils, teachers, peripatetic staff, volunteers, parents or carers and visitors who have access to and are users of our school ICT systems, both in and out of the school.

**Roles and Responsibilities for Online safety**

The ICT/Online Safety Co-ordinator will be the central point of contact for all safety issues within the school, ensuring that policies are current and adhered to, any breaches or abuse will involve sanctions and will be reported to the Principal and the Governors. Alongside this we adopt a whole school approach to ensure the safe, healthy, acceptable and effective use of the Internet and other digital technology tools in our school.

The following section outlines the online safety roles and responsibilities of individuals and groups within St. Joseph’s

**The Board of Governors**

The Board of Governors are responsible for the adoption of the Online Safety Policy and for reviewing the effectiveness of the policy.

**The Principal**

The Principal, Mrs McMullan, has a duty of care for ensuring the safety (including online safety of members of the school community) though the day to day responsibility for online safety will be delegated to the ICT Co-ordinator (Acting ICT Coordinator – Mrs McMullan). Mrs McMullan has also the responsibility for managing emails e.g. if emails are quarantined for a particular reason then she liaises with C2k to have them released.

The Principal and Senior teacher are responsible for ensuring that the ICT Coordinator, and other relevant staff, receive appropriate training to enable them to carry out their online safety roles and train their colleagues, as relevant.

**The ICT/Online Safety Co-ordinator (Mrs McMullan- Acting)**

* Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies with the Designated Teacher for Safeguarding and Child Protection, Miss Joyce
* Ensures that all staff are aware of procedures that need to be followed in the event of an online safety incident taking place.
* Provides training and advice for staff regularly including during safeguarding and child protection staff training days
* Liaises with Education Authority (EA) Belfast
* Liaises with C2K technical staff
* Receives reports of online safety incidents and completes a log of incidents in the Online Safety Risk Register which can be used to inform future online safety developments
* Attends relevant meetings e.g. cluster meetings, C2k, Fronter, ICT Conferences
* Reports regularly to Principal
* Maps and reviews the School’s Online Safety curricular provision – ensuring relevance, breadth and progression.
* Monitors the impact of Online Safety education in our school and if necessary to fill any gaps.
* Raises and manage new initiatives including annual initiatives such as anti-bullying week and Safer Internet Day
* Produces, monitors and reviews St. Joseph’s PS Online Safety Policy
* Monitors network incident logs
* Monitors incidents and establish the best way of dealing with them
* Engages our school community including parents or carers and the pupils about the online safety provision
* Monitors and reviews St. Joseph’s filtering policy through liaising with C2k and approve requests for filtering changes.

**Whole School Approach**

Our consistent whole school approach to online safety involves:

* Safeguarding including Online Safety is a key priority of all teaching and non-teaching staff, volunteers, visitors and the Board of Governors.
* All teaching/non-teaching staff can recognise and are aware of Online Safety issues.
* Online Training of teaching/non-teaching staff occurs on an annual basis.
* Online safety messages are integrated across the curriculum for pupils in Nursery and all Key Stages.
* Online safety messages are distributed amongst pupils, staff, parents or carers and the wider community.
* Knowledge is shared amongst staff and there are good capacity building opportunities.
* There is on-going monitoring and evaluation of policy and practice.

**Education of Staff**

* All teaching/non-teaching staff of St. Joseph’s PS are familiar with our Online Safety Policy. Staff are trained to recognise and to be aware of and have training (led by ICT Coordinator) in online safety risks.
* Staff have read, understood and signed the St. Joseph’s PS Staff Acceptable Use Policy for C2k Managed Portable Devices (Appendix 6: EN094).
* Staff report any online safety incident to the ICT Co-ordinator, **Mrs McMullan**. (See *Procedures for Reporting and Dealing with Incidents Surrounding Breaches in the School’s Online Safety Guidelines).* In line with St. Joseph’s PS Safeguarding and Child Protection Policy, if the incident is a safeguarding/child protection this will be reported to the Designated teacher **Mr McVeigh** or Designated teacher **Mrs McMullan**.
* Circulars relating to online safety e.g. DENI Circular 2016/27 ‘Online Safety’, Circular 2016/26 Effective Educational Uses of Mobile Digital Devices, are emailed to all staff and they are saved for reference in the staff folder (ICT Documents).
* All staff implement E-safety lessons not only during E-safety week, but throughout the year.
* At meetings staff regularly share good practice in relation to online safety, e.g. sharing of websites which promote online safety.
* Staff are aware that all digital communications with pupils and parents or carers should be on a professional level and only carried out using official school systems e.g. use of School Website, Fronter, Google Classroom and See Saw app.
* Internet use should be planned, task orientated and educational within a regulated and managed environment. It is best practice that pupils should be guided to sites checked as suitable for their use.
* Supervision is a key strategy, where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the pupils visit.
* Staff discuss with pupils the rules for responsible internet use as pupils need to be taught how to be internet wise and learn how to recognise and avoid potential risks. Staff recognise that pupils need to know how to respond to inappropriate material (SMART rules are displayed in ALL classrooms).
* Staff should act as good role models while using digital technologies, the internet and mobile devices.

In St Joseph’swe understand that although they are invaluable resources, digital technologies present risks and benefits and therefore the education of pupils in online safety is an essential part of St. Joseph’s PS online safety provision. We aim to teach our children appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. Pupils need the help and support of the school to recognise and avoid online safety risks and help build their resilience.

* Pupils will be directed to a “Three way agreement for Online Safety” this is discussed in school and at home before they sign to show agreement of the terms.
* (Appendices 2a, 2b and 2c)
* Pupils are taught how to adopt safe and responsible use of digital technology both in and outside school. All pupils are familiar with our Anti Bullying Policy which includes reference to online bullying.
* While using the Internet at school, pupils **should, where possible**, be supervised directly by a member of staff. Independent electronic research requires specific teacher permission and research must be conducted in designated curricular areas only. In all cases, pupils should be reminded of their responsibility to use these resources in line with the school policy on acceptable use.
* We actively promote online safety messages for pupils on how to stay safe, how to protect themselves online and how to take responsibility for their own and others’ safety. We teach them how to make good judgements about websites and e-mails received (see flowchart for responding to e-safety incidents)
* Childnet International SMART Posters (www.kidsmart.org.uk) are displayed around the school to help reinforce safety messages for pupils. Materials from outside agencies are also distributed to pupils for use in school or at home with their parents.
* Uploading information – know what is safe to upload and not upload personal information e.g. Real name, home/email address, mobile/landline phone numbers, friends name and details, specific interests or clubs attended.
* Online safety lessons are integrated by staff across the curriculum for pupils in Foundation Stage, Key Stage One and Key Stage Two. Standalone online safety lessons are incorporated into PDMU lessons, Safer Internet Day activities and school assemblies. We enter competitions organised by agencies such as EA/C2k.
* There are links to online safety websites(CEOP) on the Homepage and in the Class Zone section of our School Website that pupils access both in school and at home with their parents/carers (https://www.stjosephstyrella.com/class-zone/p4/)
* Outside agencies e.g. NSPCC and the PSNI are used to reinforce the online safety messages from P1 - 7.
* St. Joseph’s pupils understand the importance of reporting abuse, misuse or access to inappropriate materials and know the procedures to follow. They are reminded of these during school assemblies.
* St. Joseph’s pupils are taught how to conduct online research safely and effectively and they understand the need to respect copyright when using material accessed on the internet.

**Education of Parents or carers and Wider Community**

St. Joseph’s parents/carers play a crucial role in ensuring that their children understand the need to use the internet/digital devices safely, in an appropriate way and in the monitoring of their on-line behaviours. Parents and carers may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure how to respond.

The school will therefore help provide Online Safety information and awareness to parents or carers through:

* website links (swgfl.org.uk, [www.saferinternet.org.uk](http://www.saferinternet.org.uk), <http://childnet.com/parents-and-carers>, https://www.thinkuknow.co.uk/
* sending messages through our school app about current online concerns in games/apps
* Providing information/access to workshops from outside agencies e.g. NSPCC, PSNI
* Information on High profile campaigns e.g. Safer Internet Day (Term 2 each year)

Both parents and children annually sign our Pupil Acceptable Use of the Internet and School-Based Digital Technology including Mobile Digital Devices *(See Appendices 2a, 2b and 2c).*

All parents/carers sign our *Consent Form for Digital Images* that allows their child’s images to be used:

* Within the school for display purposes
* Externally for displays associated with the school
* By local, national, television and press
* On St. Joseph’s PS website
* On the St. Joseph’s PS Twitter account (2019)

Parents have the choice to opt in or out of any of the above. Should a parent change their mind regarding permission for their child’s image to be used, they are asked to put this in writing and inform the School Office so that records can be amended.

St. Joseph’s PS take every opportunity to help parents or carers understand online safety issues through parents’ curriculum evenings, NSPCC workshops, newsletters, assemblies, School Website and information regarding national or local online safety campaigns and literature.

We advise St. Joseph’s PS parents/carers to take the following action when taking digital images of pupils in and around the school:

* Digital and video images may be taken at school events providing these are not uploaded to social media e.g. Facebook, Twitter, WhatsApp, Instagram, Snapchat
* **Use of the internet**
* Through the internet, school and their pupils have access to a vast up-to-date global network of information and resources. They can communicate with others (including video conferencing) and publish information. The educational value of appropriate use of information / resources and the ability to communicate and publish information on the Internet is substantial. This worldwide system of computer networks is not governed by any entity. There are also no limits or checks on the kind of information that is maintained by, and accessible to, Internet users. C2K/Capita provides the school with hardware, software and connectivity to access the internet, which is controlled by a filtering mechanism. Use of the internet is monitored by C2k/Capita and incidents are reported to the Principal. The internet filtering by C2K/Capita is based on Websense Services which categorise websites for access / no access. This occurs on a daily basis therefore blocking access to newly created websites if deemed inappropriate.
* We teach our children and young people how to use the Internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding and communicating effectively in order to further learning, through ICT and/or PDMU lessons.

**Service Providers, Technical – infrastructure / equipment, filtering and monitoring**

St Joseph’s PS has a managed ICT service provided by C2k. It is our responsibility to ensure that the service provider (C2k) carries out all the online safety measures that would otherwise be the responsibility of the school.

C2k regularly monitor our network for any misuse or attempted misuse which can then be reported to the Principal or Online Safety Co-ordinator. C2k ensures that the school meets recommended technical requirements. They regularly review and audit the safety and security of our school system. Servers, wireless systems and cabling is securely located and physical access is restricted. All users have clearly defined access rights to school technical systems and devices (See Register of Access List). All users are provided with a username and secure password by the Network Manager (Mrs McMullan) who keeps an up to date record of users and their usernames. Staff and pupils are responsible for the security of their username and password and will be required to change their password every 3 months. The ‘C2k Manager’ password for our school network used by the Network Manager (Mrs McMullan) is available to the Principal (Mrs McMullan).

The managed service provider (C2k) is aware of:

* DENI Circular 2016/27 “*Online Safety*”
* DENI Circular 2016/26 *“Effective Educational Uses of Mobile Digital Devices”*

**Monitoring and Evaluating**

As part of our Safeguarding Policy, breaches of online safety are recorded in an Online Safety Risk Register kept by the Designated Teacher (Mr McVeigh), together with the Safeguarding and Child Protection records in a locked filing cabinet.)

The Online Safety Policy is reviewed annually or amended accordingly if new circulars are issued. If changes are to be made all staff are consulted.

**Procedures for Reporting and Dealing with Incidents Surrounding Breaches in the School’s Online Safety Guidelines** *(See flow chart in Appendix).*

In line with our Safeguarding and Child Protection Policy, we have robust channels of communication in place for reporting online safety issues. Pupils and staff know who they can turn to if there is a problem. Instances relating to Safeguarding and Child Protection should be communicated to the designated teacher Mr McVeigh. More advice is available if required in the Safer Internet Area within Fronter. In cases of Internet abuse, or where a pupil is at risk, our safeguarding and child protection procedures will be implemented.

The school will, if necessary; inform parents or carers of incidents of inappropriate Online Safety behaviour that takes place in our school, or outside school if it involves members of our school community.

If there is an online safety incident, the action taken depends on whether unsuitable materials were involved or if there were illegal materials or activities found or suspected.

In the first instance if unsuitable material is found:

* This is reported to the ICT Co-ordinator Mrs McMullan.
* The ICT Co-ordinator assesses the material and discusses it with the persons involved (staff or pupils) and decides upon an appropriate course of action.
* Mr McVeigh will record details in the Online Safety Risk Register and may if necessary consult with the DT or DDT. If appropriate the DT or DDT will consult with the Safeguarding and Child Protection Team at the Education Authority.
* Mr McVeigh liaises with the Principal to discuss the incident.
* Following this assessment, the policy may be reviewed and changed if lessons have been learned.
* If illegal materials or activities are found or suspected, *which pose no immediate risk to pupils*; the above procedures will be followed and it will be reported to CEOP (Child Exploitation and Online Protection.)
* The evidence must be secured and preserved.
* The school then awaits a response from CEOP or from the police.
* If no illegal activity or material is confirmed, we revert to our internal procedures.

If the incident is more serious:

* If illegal activity or materials are confirmed, police or relevant authorities complete their investigation and seek advice from relevant professional bodies.
* In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action.
* If illegal material or activities are found, or are suspected, that pose immediate risk:
* The member of staff or Mrs McMullan reports this to CEOP and to the Designated Teacher or the Deputy Designated Teacher who follow St. Joseph’s PS Safeguarding and Child Protection Procedures.
* The evidence must be secured and preserved.
* The school then awaits a response from CEOP or from the police.
* If illegal activity or materials are confirmed, police or relevant authorities complete their investigation and seek advice from relevant professional bodies.
* In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures being implemented whilst there is on-going police action.

**How will E-Safety/Online complaints be dealt with?**

Misuse will be dealt with by a member of Senior Leadership Team. Staff misuse will be dealt with by Principal. Complaints about the Principal’s misuse will be referred to Vice Principal or Chair Person of Board of Governors. Potential child protection or illegal issues will be dealt with by Designated Child Protection Officer with school authority and CEOP involved as necessary.

Sanctions will be linked to school Behaviour Policy. Staff and pupils will be made aware of the flowchart for responding to e-safety incidents. ***(Appendix )***

**Information Security**

Security of the school information system will be maintained by C2K/Capita. Virus protection performs checks and updates regularly. Portable media devices are used with permission and virus checks occur automatically on these. Internet use is monitored. Filtering / blocking of websites and email may also occur.

**Location and Supervision**

a) Rules for digital technology use will be displayed in all classrooms and around the school.

b) Internet access for pupils at St Joseph’s Primary School is located in the classrooms and in resource areas. All such machines are in full view of people circulating in the area.

c) Users will be made aware that the ICT Co-ordinator and Principal have the ability to review files and communications to ensure that users are using the system responsibly. All uses of the Internet are logged and all sites visited by individual users are recorded. While normal privacy is respected and protected by password controls, as with the Internet itself, users must not expect files stored on school servers to be absolutely private.

At St Joseph’s Primary School we expect good behaviour on the internet just as we do in the classroom or school corridor. This includes materials they choose to access and language they use.

**Pupils must ask permission before accessing the Internet**.

Access to the Internet requires parental permission and a signed declaration by pupils agreeing to the school rules for use of the Internet. (***see*** ***Three way agreement for Safe***, ***Effective and Acceptable Use of the Internet and Digital Technologies / E Safety***)

The Internet is provided for pupils to conduct research and communicate with others. Planned activities should have the potential to enrich and extend learning. While the use of information and communication technologies is a required aspect of the statutory Northern Ireland Curriculum, access to the Internet remains **a privilege and not a right**. It is given to pupils who act in a considerate and responsible manner, and should be withdrawn if they fail to maintain acceptable standards of use. Use of the computer system without permission or for inappropriate purposes could constitute a criminal offence under the computer Misuse Act 1990.

During school hours or for home learning activities that require internet access the teachers will guide pupils towards appropriate materials. Outside school hours families bear responsibility for such guidance – just as they exercise control with information sources such as television, telephones, movies, radio, and other potentially offensive media they must do the same with the Internet.

**Browsing / Using Search Engines**

Our school does offer protection with the supervision of children and a filtering software system is installed but this software is not always foolproof. Neither the school nor C2K/Capita can accept liability for materials accessed or any consequence of internet access. Adult supervision of children’s ICT use is preferable; it is not always realistic or practical outside school. We must therefore alert children to the risks they might encounter and help them to develop a safe, healthy, acceptable and effective use of the Internet which can be used in any setting – school or home.

Children must be empowered with the knowledge of how to deal with situations they may encounter. ***(Also see flow chart for reporting e-safety incidents – Appendix A***, ***A1 and A2)***

When registering on a website in school or for school purposes, school details such as address, email address and phone numbers must be used. Not staff or pupils personal information. Access to websites should enhance the pupils learning experience.

Pupils using search engines are expected not to deliberately seek out offensive materials. Should any pupil encounter such material accidentally, they should report it immediately to a teacher.

When using the Internet at St Joseph’s Primary School, all users must comply with all copyright, libel, fraud, discrimination and obscenity laws. Children must be aware that plenty of the material available on the internet is correct information however there is also incorrect information. Children need to consider the author of the material, date it was created and the content. Like books information from the internet must not be plagiarised. With such vast amounts of information available on the internet search tools provide the opportunity to locate specific information quickly and easily. The search results will turn up a huge number of sites containing the keyword information.

**Using Email**

Email is a means of communication, messages can be sent over the internet to anywhere or anyone in the world. Text, images, pictures, sound, animations or movies can be attached to an email.

Like any business schools see email as a valuable tool for the communication of information, in St Joseph’s Primary School staff use it daily.

Email has the potential to help with literacy skills – spelling accuracy (emails will not send if address is spelt incorrectly), language succinctness (emails should be brief and clear) presentation (typed text- clear to read) and another means of communication other than verbal. We encourage the use of email for communication between colleagues in schools and industry. Emails sent to external organisations must be carefully written and authorised before sending in the same way as a letter on school headed paper.

Messages will be analysed by C2k/Capita. Email considered inappropriate will be held and only released by the C2K mail manger. Messages may be held because of spam / oversized attachments / racial, sexual and profanity terms used / encrypted mail / inappropriate images / executables and banned file types.

Despite an email filtering system unwanted emails (spam / spoofing emails) may still get through. These unwanted emails may contain inappropriate content which is received or sent to the user’s entire address book, they may be hiding a virus or obtain sensitive information from a user’s account. Other terms linked to this include phishing and pharming – tricking people into revealing information / data. Other types of unwanted emails include:

* Angry / abusive emails– some times called flaming
* Bullying / harassment emails
* Bombing emails– a large message or number of messages that causes the user’s email program to crash
* Email as a form of communication continues to grow in popularity, we must make children aware of the unpleasant side to emails mentioned above and prepare them to deal with emails effectively to protect the school’s network against viruses. In St Joseph’s, children will be taught the appropriate tone and language to use. Children will be made aware that they need to think and evaluate the source of emails and attachments. If they receive abusive or bullying messages to seek help from an adult (teacher, parent or carer) and they must not respond to the message.

Any information they find or receive that has content or contact that makes them feel uncomfortable should be reported to an adult immediately. Spam or junk messages should not be opened, responded to and should be deleted. Personal information must be kept private.

Some webmail providers allow email addresses to be shared with third parties. Many offer effective email filtering tools which many be optional setting that needs selected, therefore pupils are not permitted to use any other e-mail service in school except the one provided by C2k/Capita.

**Password Protocol**

All children in St Joseph’s will be allocated a user name by C2k. The ICT Coordinator will also keep a copy of this document, as system administrator. Pupils will use only their own network login and password.

GUIDELINES ON IPAD USE

**Care of iPad**

* User must use protective covers/cases for their iPad.
* The iPad screen is made of glass and therefore is subject to cracking and breaking if misused: Never drop or place heavy objects (books, laptops, etc.) on top of the iPad.
* Only a soft cloth or approved laptop screening solution is to be used to clean the iPad screen.
* Do not subject the iPad to extreme heat or cold.
* Do not store or leave unattended in vehicles.
* You will not ‘jailbreak’ the device.
* In the case of loss, theft or other damage occurring outside of school, users accept full responsibility to repair, replace or make good the ipad to its original state.

**Acceptable Use**

* Use of the iPad should be considered the same as any other technology tool provided by the school.
* The user will abide by the schools Internet Acceptable Usage policy with regard to iPad usage.
* E-mail list of apps needed to ICT co-ordinator and they will consult the principal before purchasing.
* To ensure that all apps meet with the requirements of the schools Internet Safety- AUP (Acceptable Usage Policy) and ICT Policy.
* To inform the ICT co-ordinator of any apps that do not meet said requirements and remove them from your device.
* The iPad will not be synched or attached to your home or personal computer.
* To not use the device to store personal documents such as video or audio material other than which is directly related to your school needs.
* Use of the camera only permitted in line with the Child Protection Policy.
* You will not remove profiles or restrictions placed on the device.

**Security**

* To not allow any pupil to use the iPad for any purpose except for curricular purpose under a controlled environment in the presence of a member of staff

**Safeguarding and Maintaining as an Academic Tool Each iPad**

iPads should be charged and ready to use in school every day. When the iPads are charging they will be saving all information onto iCloud. Any items that are deleted from the iPad cannot be recovered. The memory space on the iPads, are limited, so only school documents/materials should be stored. Each member of staff should know the whereabouts of their iPads at all times. It is their responsibility to ensure that the iPad is kept safe and secure. If an iPad is found unattended, it should be given to the ICT co-ordinator straight away.

**Lost, damaged or Stolen iPad**

If the iPad is lost, stolen or damaged, the ICT co-ordinator should be notified immediately. IPads that are believed to be stolen can be tracked through iCloud.

**Prohibited Uses of iPads**

* Accessing Inappropriate Materials – All material on the iPad must adhere to the ‘Internet Safety – An Acceptable Usage of the Internet.’ Users are not allowed to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.
* Illegal Activities- Use of the school’s internet/ e-mail accounts for financial or commercial gain or for any illegal activity.
* Violating Copyrights- Users are not allowed to have music and install apps on their iPad. An email should be sent with relevant apps to the ICT co-ordinator who will ask permission from the Principal/Vice Principal.
* Cameras- Users must use good judgement when using the camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way. Any use of camera in toilets or changing room, regardless of intent, will be treated as a serious violation.
* Images of other people may only be made with the permission of those in the photograph.
* Posting of images/movie on the Internet into a public forum is strictly forbidden, without the express permission of a member of the Senior Management team.
* Use of the camera and microphone is strictly prohibited unless permission is granted by a teacher.
* Any user caught trying to gain access to another user’s accounts, files or data will be subject to disciplinary action.
* Any attempt to destroy hardware, software or data will be subject to disciplinary action.
* Jail breaking is the process which removes any limitations placed on the iPad by apple. Jail breaking results in a less secure device and is strictly prohibited.
* Inappropriate media may not be used as a screensaver or background photo. Presence of pornographic materials, inappropriate language, alcohol, drug or gang related symbols or pictures will result in disciplinary actions.
* Individual users are responsible for the setting up and use of any home internet connections and no support will be provided for this by the school.
* Users should be aware of and abide by the guidelines set out by the

‘E-Safety Policy- An Acceptable Use of the Internet.’

* The Principal/Vice Principal/Designated teacher reserves the right to confiscate and search an iPad to ensure compliance with this acceptable Use of Internet Policy.



**Adult Users must read and sign below:**

I have read, understand and agree to abide by the terms of the iPad and ICT Acceptable Use Policy.

|  |
| --- |
| Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |



**Adult Users must read and sign below:**

I have read, understand and agree to abide by the terms of the iPad and ICT Acceptable Use Policy.

|  |
| --- |
| Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |



**Student Pledge for iPad Use.**

* I will take good care of the iPad.
* I will never leave the iPad unattended.
* I will keep food and drinks away from the iPad since they may cause damage to the device.
* I will not remove any part of the iPad or attempt any repairs.
* I will use the iPads in ways that are appropriate.
* I understand that the iPad is subject to inspection at any time and without notice.
* I will only use the camera or the microphone with my teacher’s permission.
* I will only photograph/ audio record people with their permission.

I agree to abide by the statements of this iPad acceptable use policy.

|  |  |
| --- | --- |
|  | Pupil Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | Class: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | Pupil Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | Parent Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | Date: \_\_\_\_\_\_\_\_\_\_ |

**An Acceptable Use of the Internet**

With the installation of C2K computers, interactive whiteboards and iPads in classrooms, children and teachers now have increased access to the Internet. There is a need to provide pupils with as safe an Internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.

It is therefore important that schools have in place an Internet Safety policy with clear rules for an acceptable use of Internet resources.

It is essential that teachers, parents, Board of Governors and pupils are all aware of Internet safety of all users.

What is the Internet?

The Internet is a huge network of computers making a worldwide community. It is a way of connecting computers together so that peope using them can:

* talk to each other
* send and receive messages
* obtain information and resources
* publish information
* buy and sell things
* have fun

Its most frequently used facilities include:

**The World Wide Web (www)**

The World Wide Web (www) or Web provides easy access to the vast quantity of information and resources available on the Internet and is the facility which people use to ‘surf’ for information. It is made up of millions of screens or pages of information.

The collection of pages created by one individual or organisation is known as a website. Each page can include text sound, images, animation and video and has its own unique address.

**E-Mail**

E-mail allows users to send and receive written messages.

**Chat Rooms**

Chat rooms allow a number of people to ‘meet’ on the Internet. It is similar to having a telephone converstaion with a number of people at one time except that the participants type instead of talk.

The Internet is often described as being like a vast city. It is an exciting place with a great variety of places to visit. There are shops, entertainment areas, educational areas and people to meet. But it also contains dangers. There are areas that we do not want to go to and that we certainly would not want children to visit.

How valuable is the Internet in Education?

The Internet is an unique and exciting resource. It brings the world into the classroom by giving children access to a global network of educational resources.

* It gives children opportunities to locate, retrieve and exchange information.
* It encourages the development of ICT skills that are vital to life-long learning.
* It takes learning beyond the classroom.
* It allows access to stores of information that might otherwise be unavailable in school.
* It provides up-to-date information.
* It is a fast and efficient way of communicating and retrieving information.
* It encourages independent learning.
* Children enjoy using it.
* It is part of their life experience. It is ‘cool’.

The Internet is increasingly forming part of our work, home, social and leisure activities. There is no doubt that the use of the Internet is an essential skill for children as they grow up in the modern world.

What are the Dangers?

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restrictions. This brings young people into contact with people from all sectors of society and with a wide variety of materials some of which could be unsuitable.

Key Concerns are:

* **Content Risk-** Children may be exposed to harmful material. Through the Internet there are unsuitable materials in many varieties. Anyone can post material on the Internet. Some material is published for an adult audience and is unsuitable for children e.g. materials with a sexual content. Materials may express extreme views. E.g. some use the web to publish information on weapons, crime and racism which would be restricted elsewhere. Materials may contain misleading and inaccurate information E.g. some use the web to promote activities which are harmful such as anorexia and bulimia.

Children need to be taught:

* That information on the Internet is not always accurate or true.
* To question the source of information
* How to respond to unsuitable materials or requests and that they should tell a teacher/adult immediately.
* **Contact Risk-** Children may participate in adult initiated online activity.

Some adults use chat rooms or e-mails to communicate with children for

inappropriate reasons. Children may come into contact with someone on-line who may wish to harm them.

Children need to be taught:

* That people are not always who they say they are.
* That ‘Stranger Danger’ applies to the people they encounter through the Internet.
* That they should never give out personal details or
* That they should never meet alone anyone contacted via the Internet.
* **Conduct Risk-** Children may become a perpetrator or victim in peer-to-peer exchange. Children need to be aware of the impact that their online activity can have on both themselves and other people, and the digital footprint that they create on the internet.

Children need to be taught:

* To keep their personal information safe.
* That people are not always who they say they are.
* That the information they have posted may be viewed and potentially shared with others at a later date.
* How to report inappropriate conversations, messages, images and behaviours.
* **Commercial Risk-** Children may become exposed to inappropriate commercial advertising, marketing schemes or hidden costs.The Internet is a powerful vehicle for advertising. In visiting websites children have easy access to advertising which is very persuasive.

Children need to be taught:

* Not to fill out forms with a lot of personal details.
* Not to use an adults credit card number to order online products.

If children are to use the Internet in places other than at school e.g. libraries, clubs and at home, they need to be educated about how to behave on-line and to discuss problems.

*There are no totally effective solutions to problems of Internet safety. Teachers, pupils and parents must be vigilant.*

Steps We Take to Protect Children in School

**Use of a Filtered Service**

Access to the Internet on computers and laptops is provided through a filtered service. All access is provided through the C2k service which is designed to filter out unsuitable materials. Access to the Internet on iPads is provided through a filtered service provided by iTeach.

**Planned Activities**

Use of the Internet is a planned activity. Aimless surfing is not allowed. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.

Websites are previewed by teachers and revisited to ensure that they are suitable for children’s curriculum needs and ability levels.

Search engines are used selectively. Teachers will choose the search engine and topic and discuss sensible search words which have been tried out beforehand.

**Restrictions on E-mail**

KS2 children are given individual web based e-mail addresses. These accounts are filtered by Capita. The children would only be accessing emails when supervised by teacher/adult.

**Use of Agencies: PSNI; CEOPS; SWGFL**

Our pupils are regularly instructed on how to stay safe on the Internet and how to use communicative technology appropriately. Each year we celebrate Internet Safety Day and organise appropriate talks with external agencies. During curriculum meetings we provide information to parents on how to stay safe on the internet. Our P7 children also participate in the PSNI Bee Safe programme. Staff of St Mary’s follow the recommendations from The Safeguarding Board (Northern Ireland) Act and use the SWGFL ‘360 degree safe’ online safety self-assessment tool to help review their online safety policy and practice.

**Internet Safety Rules**

Children are taught to be Internet Wise (netiquette). Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material.

Children and their parents will be expected to agree to and sign ‘An Acceptable Internet Policy’ (Appendix 1/2) and Digital and Video Images (Appendix 3).

All reasonable and appropriate steps have been taken to protect pupils. The school recognises that despite employing safety procedures, in some circumstances, the Internet may give children access to undesirable information or images.

Children are regularly reminded that should they encounter inappropriate material on line they must immediately:

* Leave that website
* Inform an adult

Should a child or teacher encounter unsuitable material on the internet, this will be reported to the ICT co-ordinator and Principal. This information will then be logged with C2k via the C2k helpdesk number.

**Mobile Phones & Social Networking Sites**

Many mobile phones now provide access to the internet and social networking sites and for this reason and for the protection of the entire school community. We would ask parents to note that mobile phones are not permitted on school, premises unless a prior written agreement exists between parents and the Principal.

As a school we recognise that technology is fast-paced and ever-evolving. We encourage the responsible use of computers technologies as a valid communication and research tool however, we do not encourage pupils (nor legally should pupils) under 16 years become members of any social networking site.

We would strongly advise parents against allowing pupils to access sites such as Facebook or Twitter etc.

Obviously, this is a decision that parents must make and police for themselves but we, as a school, actively discourage this use until such times as pupils are mature enough to use this method of communication appropriately.

Inappropriate use of social networking sites or mobile phones which could cause offence or reflect negatively on any pupil or member of staff will be taken very seriously.

Any pupils found to be using social networking sites inappropriately (whether inside or outside school) will lose ICT privileges within school and further action, if deemed appropriate, may be taken.

Points for Teachers to Consider

Internet use should be planned, task orientated and educational within a regulated and managed environment.

* Supervision is the key strategy. Children should have a teacher or classroom assistant present when using the Internet. Computers should be positioned so that it is possible for adults to see materials on screen.
* Children should know why they are using the Internet. Aimless surfing should never be allowed. Teach children to use the Internet in response to a need e.g. to answer a question which has arisen from work in the class.
* Children do not need thousands of website addresses. A small appropriate choice is much more effective. ‘Favourites’ is a useful way to present this choice. Sites should always be previewed and revisited to be checked out. Consider off-line viewing.
* Discuss with pupils the rules for responsible Internet use. It is not enough to protect children from materials; we must teach them to become Internet Wise. Children need to learn to recognise and avoid the risks. Children need to know what to do if they come across inappropriate material or if they approached by a stranger.
* They should ensure that the privacy settings are correct and that their account does not compromise their professional position. It is therefore essential that staff do not make any disparaging remarks about employer/colleague/ parents or pupils. Doing so in presence of others may be deemed as bullying and/or harassment. This may result in disciplinary action.
* Be informed – read e.g. NGfL Superhighway Safety. <http://safety.ngfl.gok.uk>
* Discuss Internet Safety with colleagues and as a staff.
* All members of staff are expected to agree and sign ‘A Staff Acceptable Use of Internet Policy’ (Appendix 4)

**Points for Parents to Consider**

It is important to promote Internet Safety in the home and to monitor Internet use.

* Keep the computer in a communal area in the home.
* Ask children how the computer works.
* Monitor on-line time and be aware of excessive hours spent on the Internet.
* Take an interest in what children are doing. Discuss with the children what they are seeing and using on the Internet.
* Advise children to take care and to use the Internet in a sensible and responsible manner. Know the Smart tips.
* Discuss the fact that there are websites which are unsuitable.
* Discuss how children should respond to unsuitable material or requests.
* Remind children never to give out personal information on the Internet.
* Remind children that people on line may not be who they say they are.
* Be vigilant. Ensure that children do not arrange to meet someone they meet on line.
* Be aware that children may be using the Internet in places other than in their own home or school.

**Filtering for the Home Computer**

Parents may wish to invest in security software for their children’s computers. Some of this software works by monitoring all internet activity for trigger words.

There are many types of security software available.

Examples include:

* Net Nanny [www.netnanny.com](http://www.netnanny.com)
* Cyber Patrol
* Surfwatch [www.safesurf.com](http://www.safesurf.com)
* Or parents may wish to make use of the AOL children’s selection at [www.aol.com](http://www.aol.com)

Points for Children to Consider

Follow these SMART TIPS

|  |  |
| --- | --- |
| S | **Secret** – Always keep your name, address, mobile phone number and password private- it’s like giving out the keys to your home! |

|  |  |
| --- | --- |
| M | **Meeting** someone you have contacted in cyberspace can be dangerous. Only do so with your parent’s/carer’s permission, and then when they can be present. |

|  |  |
| --- | --- |
| A | **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. |

|  |  |
| --- | --- |
| R | **Remember** someone on-line may be lying and not be who they say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there! |

|  |  |
| --- | --- |
| T | **Tell** your parent or carer if someone or something makes you feel uncomfortable or worried. |

SMART Tips from:- Helping your parents be cool about the Internet, produced by Northern Ireland Area Child Protection Committee.

On our School Website/Social Media Pages:

* Any images of children will only be uploaded with parental permission (Appendix 3)
* No close-up pictures of children will be made available online.
* Children and teachers will not reveal their personal details, home addresses or telephone numbers on the website.
* Website links selected by teachers, (with prior approval from Principal/ Vice Principal) may be put on the website for pupils to access outside of school- sites will be previewed and checked regularly.

Parents’/Carers’ permission will be sought to publish pupils work and/ or photographs. These will only be published subject to the strict safeguards above.

**Guidance Material on Internet Safety**

DE Circular 2017/04- Safeguarding and Child Protection in Schools – A Guide for Schools

DHSPSS Co-operating to Safeguard Children and Young People in Northern Ireland (2016)

DE Circular 2016/27- Online Safety

DE Circular 2013/25-eSafety guidance

DE Circular 2011/22- Internet Safety guidance

DE Circular 2007/01- Acceptable use of the Internet and digital technologies in schools

Child Exploitation and Online Protection (CEOP)

[www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

NSPCC Internet Safety Training

[www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-children-safe-online-course/](http://www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-children-safe-online-course/)

Examples of advice for staying safe online for children are also available from:

[www.saferinternet.org.uk/advice-centre/young-people/resources-3-11s](http://www.saferinternet.org.uk/advice-centre/young-people/resources-3-11s)

[www.getsafeonline.org](http://www.getsafeonline.org)

Monitoring and Evaluating Policy

The ICT Policy will be reviewed annually by the On-line Safety Team.

The policy’s effectiveness will be evaluated in the event of a change of legislation or training.

|  |  |  |
| --- | --- | --- |
| Last Reviewed | November 2018 |  |
| Reviewed |  | Updated to:  Reference the circulars consulted in developing the policy  DE Circular 2017/04- Safeguarding and Child Protection in Schools – A Guide for Schools  DHSPSS Co-operating to Safeguard Children and Young People in Northern Ireland (2016)  DE Circular 2016/27- Online Safety  DE Circular 2013/25-eSafety guidance  DE Circular 2011/22- Internet Safety guidance  DE Circular 2007/01- Acceptable use of the Internet and digital technologies in schools |
| Date Ratified by BoG: |  |  |
| Date of next Review: |  |  |

(APPENDIX 1)

ICT Code of Practice Agreement for Pupils and Parents

The school has installed computers, iPads and internet access to help our learning. These rules will keep everyone safe and help us to be fair to others.

* I will access the system with my login and password, which I will keep secret.
* I will not access other people’s file without permission.
* I will ask a teacher or a suitable adult if I want to use the computers.
* I will ask permission from a member of staff before using the Internet.
* I will only use the computers for school work and homework.
* I will take care of the computer and other equipment.
* I will ask for help from a teacher or a sensible adult if I am not sure what to do or if I think I have done something wrong.
* I will not bring an iPad, phone or technological device into school without permission.
* I will only e-mail people I know, or my teacher has approved.
* I will not open e-mails sent by someone I don’t know.
* The messages I send will be polite and responsible.
* I will not give my home address or telephone number, or arrange to meet someone.
* I will tell a teacher or suitable adult if I see something that upsets me on the screen.
* I will report any unpleasant materials or messages sent to me.
* I understand that the school may check my computer files and may monitor the Internet sites I visit.
* I will not use Internet chat-rooms in school.
* I will never give out personal information or passwords.
* I know that if I break the rules I might not be allowed to use a computer.

|  |  |  |
| --- | --- | --- |
| Signed by child |  |  |
| Signed by parent/guardian |  |  |
| Date |  |  |

APPENDIX 2

ICT Code of Practice Agreement for Individual Pupils who have access to an iPad as a recommendation from the Statement of Needs,

To help ensure that e-learning is successful and safe, we ask you to commit to the principles outlined in this agreement. As a school we are prepared to provide the support and resources necessary to make this work, but we also require the commitment of parents and pupils.

As you read through this leaflet you will see a summary of the e-learning commitment that the school is making to the pupils, and to you as parents. It also outlines the commitment that will be needed from the home, and from the children themselves, to make this work.

When you have read these sections please sign the agreement. This will help to ensure that we are all working together to achieve success.

THE SCHOOL WILL…

● Give the pupil an introduction to using and caring for the iPad.

● Teach pupil to use the iPad safely.

● Monitor the use of the iPad both remotely and directly in and around school.

AT HOME WE WILL…

● Ensure that our child understands how to care for and protect their iPad.

● Report any faults with the iPad promptly.

● Understand that the iPad remains the property of individual and as such should be respected.

● Make sure the iPad is not used for any illegal and/or anti-social purpose, including access to inappropriate Internet sites and chat rooms.

● Ensure that our child understands that the device is important for educational purposes.

● Ensure that Apps and resources that are provided by the school are not removed from the iPad.

● Remind our child to bring it to school each day.

● Understand that the iPad may be inspected by the teacher upon request and that the iPad and its contents (whether created at home or school) can be viewed by the teacher at any time.

● Take responsibility for any inappropriate use of the iPad at home.

AS A PUPIL I WILL…

● Look after the iPad very carefully all the time.

● Ensure it is within a case when at school.

● Not use the iPad for any form of cyber-bullying, harassing, insulting or attacking others.

● Bring it to school every day.

● Transport the iPad as securely as possible (e.g. not visible in a vehicle; not advertise ownership of my iPad).

● Ensure that the iPad is only used for educational purposes whilst in school.

● Make sure the iPad is not used for illegal and/or anti-social purpose.

● Not physically decorate, customise or graffiti the iPad or its case.

● Allow staff to access the iPad to check for materials at any time.

● Not download apps without teacher permission.

● Not take photographs or movies without the permission of the person.

● Not upload photos/movie from the iPad to online media sharing sites, such as Facebook, YouTube etc or a public space on the Internet.

● Be mindful of the time that I spend on my iPad. I will always act on the advice of the school in the use of this advice.

PLEASE SIGN AND RETURN THIS TO THE SCHOOL AS SOON AS POSSIBLE:-

PUPIL’S AGREEMENT

I agree to abide by these terms in my use of the iPad

Name: ……………………………………………

Class: ……………………………………………

Signed: …………………………………………

Date: ……………………………………………

PARENT’S/CARERS AGREEMENT

I agree to my child having the use of the iPad on these terms

Name: ……………………………………………

Signed: ……………………………………………

Date: ……………………………………………

PRINCIPAL’S AGREEMENT

I agree on behalf of the school to provide an iPad on these terms

Signed: ……………………………………………

Date: ……………………………………………

Terms and Conditions

Failure to take such reasonable care or to abide by the other conditions listed in this document may result in the user not being able to use the iPad at home. Persistent misuse or failure to adhere to the conditions may result in the iPad being kept at school and not allowed at home.

The school will not be responsible for any outcomes which may occur if guidelines are not followed.

The iPad should be re-charged at home overnight, but the school cannot accept responsibility for the electrical costs involved.

The iPad (and software, services and applications provided by the school) will remain the property of the school.

(APPENDIX 3)

**Digital and Video Images of Pupils Agreement**

I have read the school’s Acceptable Use of the Internet and Digital Technologies policy and have circled below how I wish images of my child to be used.

|  |  |  |
| --- | --- | --- |
| Images of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (pupil’s name)  may be published in the following ways | | |
| On the school web site | Yes | No |
| On the school social media pages (twitter/facebook) | Yes | No |
| In the school prospectus/flier | Yes | No |
| In the press | Yes | No |
| For displays within school | Yes | No |

|  |
| --- |
| Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (Parent/Guardian)  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

(APPENDIX 4)

**Staff Acceptable Use Policy Agreement**

* I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.
* I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT.
* I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

**For my professional and personal safety:**

* I understand that the school will monitor my use of the ICT systems, email and other digital communications.
* I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE, iPads etc) out of school, and to the transfer of personal data (digital or paper based) out of school
* I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
* I will not disclose my username or password to anyone else, nor will I try to use any other person’s username and password.
* I understand that I should not write down or store a password where it is possible that someone may steal it.
* I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to the appropriate person.

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

* I will not access, copy, remove or otherwise alter any other user’s files, without their express permission.
* I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
* I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school’s policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
* I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
* I will not engage in any on-line activity that may compromise my professional responsibilities.
* I will not accept any friend requests from pupils.
* I will always ensure that I have watched completely any videos downloaded from sites such as ‘You Tube’ prior to use, to ensure they are appropriate.
* I will not use personal email addresses during contact teaching time.
* I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
* I will ensure that my data is regularly backed up
* I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
* I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
* I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer.
* I will not disable or cause any damage to school equipment, or the equipment belonging to others.
* I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
* I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

* I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
* I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and Principal and in the event of illegal activities the involvement of the police.
* I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date