

# Constantine Primary School - E-Safety Policy

## Content

Background / Rationale

Development, monitoring and review of the Policy

Schedule for development, monitoring and review

Roles and Responsibilities

- *Governors*
- *Headteacher*
- *E-Safety coordinator*
- *Teaching and Support Staff*
- *Pupils*
- *Parents / Carers*

Policy Statements

- *Education -Pupils*
- *Education - Parents / Carers*
- *Education and training - Staff*
- *Training - Governors*
- *Technical - infrastructure / equipment, filtering and monitoring*
- *Communications*
- *Unsuitable / inappropriate activities*
- *Responding to incidents of misuse*

Appendices:

- *Pupil Acceptable Use Policy*
- *Staff Acceptable Use Policy*

## Background / Rationale

The use of ICT in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- *Access to illegal, harmful or inappropriate images or other content*
- *Unauthorised access to / loss of / sharing of personal information*
- *The risk of being subject to grooming by those with whom they make contact on the internet.*
- *The sharing / distribution of personal images without an individual's consent or knowledge*
- *Inappropriate communication / contact with others, including strangers*
- *Cyber-bullying*
- *Access to unsuitable video / internet games*
- *An inability to evaluate the quality, accuracy and relevance of information on the internet*
- *Plagiarism and copyright infringement*
- *Illegal downloading of music or video files*

- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / pupils' resilience to the risks to which they may be exposed, so that they have the understanding, confidence and skills to face and deal with these risks.

## Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a working group made up of:

- School E-Safety Coordinator
- Headteacher
- Teachers
- Governors

## Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Governing Body on:	11.12.2012
The implementation of this e-safety policy will be monitored by the:	E-Safety Coordinator, Headteacher, Governing Body, E-Safety committee
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	September 2016
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LA ICT Manager LA Safeguarding Officer Police Commissioner's Office

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Netsweeper reports of internet activity (including sites visited)
- Surveys / questionnaires of
  - Pupils (e.g. Ofsted "Tell-us" survey / CEOP ThinkUknow survey)
  - Parents / carers
  - Staff

# Roles and Responsibilities

## Governors:

Governors are responsible for the approval of the E-Safety Policy (on the recommendation of the E-safety committee) and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- reporting to Governors

## Headteacher

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator
- The Headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant

## E-Safety Coordinator:

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority when necessary
- liaises with the school's ICT support providers to ensure that the school's ICT infrastructure is secure
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- keeps up to date with relevant E-Safety information in order to effectively carry out their e-safety role and to inform and update others as relevant
- Reports to the headteacher

## Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- They report any suspected misuse or problem to the E-Safety Co-ordinator and Headteacher for investigation / action / sanction

- Digital communications with students / pupils (email / blogs / social media should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in many aspects of the curriculum and other school activities
- Pupils understand and follow the school e-safety and acceptable use policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra curricular and extended school activities

## Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. At KS1 it would be expected that parents / carers would sign on behalf of the pupils and that at key stage 2, pupils and parents read and sign the document together
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

## Parents / Carers

Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy

# Policy Statements

## Education – Pupils

E-Safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of ICT / PHSE / other lessons and is regularly revisited - this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities, including annual involvement National E-Safety day
- Pupils should be taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms and displayed on log-on screens
- Staff should act as good role models in their use of ICT, the internet and mobile devices

## Education – parents / carers

The school will provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- Parents evenings
- Reference to the appropriate websites

## Education & Training – Staff

Staff training will be offered as follows:

- Regular E-Safety training will be made available to staff.
- New staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies (AUP)
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required

## Training – Governors

Governors will be invited to take part in e-safety training sessions, with particular importance for those who are members the E-Safety committee and child protection.

# Technical - infrastructure / equipment, filtering and monitoring

The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible. The school will take advice from NCI Technologies in this respect.

- All users (at KS2 and above) will be provided with a username and password by the e-safety coordinator. A log of the passwords and usernames will be filed in the teachers work area of the school's network. Children in KS1 will use class log-on and use of computers in this way will always be supervised by an adult. Teachers or visitors should never use a class log on for their own network access.
- Access to the school ICT systems by "guests" (e.g. volunteer helpers) onto the school system is restricted. Visitors should log on as 'visitor', with the same password, and they will not have access to areas which teachers have access to. Visitors will never use children's, staff or class log-ons

Trainee teachers will be given the same access to the schools systems as teachers with their own user name and password. They will read this policy and its appendix before using school ICT systems and sign the acceptable use agreement.

- The administrator passwords for the school ICT system, used by the ICT coordinator and NCI technicians must also be available to the Headteacher.
- The school maintains and supports the managed filtering service provided by Netsweeper.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be agreed to by the Headteacher.
- Any filtering issues should be reported immediately to the E-Safety Coordinator who will then report to Netsweeper and NCI Technologies
- Requests for sites to be removed from the filtered list will be considered by the ICT Coordinator and Headteacher. An allowed list of websites can be viewed in the Netsweeper admin area to which all teachers have access.

Websites which are filtered may be accessed by staff using a generic staff proxy. Staff are prompted to enter a username and password when using a staff proxy. Staff will keep the username and password secure and notify the head teacher and ICT coordinator if they feel the security of the password and username has been compromised. Children and visitors will never be allowed to use the staff proxy.

Staff are appropriately trained in the use of Staff Proxy used to bypass the school's filtering system. They are aware of the importance of closing web browsers after the school proxy has been used in order to prevent accidental access to unfiltered areas of the web. Staff are aware of the importance of checking websites that they may wish to access using the staff proxy first, before using them in the presence of children. The staff proxy may only be used for school/educational purposes and never for personal use.

- Staff will monitor the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Any actual, or potential, e-safety incident must be reported to the E-Safety Coordinator
- Staff use the network and ICT systems in line with the staff AUP
- The school infrastructure and individual workstations are protected by up to date virus software.

# Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies	Staff & other adults				Students / Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x							x
Use of mobile phones in lessons		x						x
Taking photos of children on mobile phones				x				x
Use of hand held devices e.g. iPads, iPods	x				x			
Use of personal email addresses in school, or on school network	X Though not recommended							x
Use of school email for personal emails	x				x			
Use of chat rooms / facilities				x				x
Use of instant messaging				x				x
Use of social networking sites, eg, Twitter	x					x		
Use of blogs	x					x		

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff are recommended to use the school email service to communicate with others when in school, or on school systems. Pupils will always do so in school and are encouraged to do so out of school.
- Users must immediately report, to the nominated person - in accordance with the school policy, the receipt of any email/communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, blog etc) must be professional in tone and content. It is recommended that these communications should only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes should not be used for these communications.
- Whole class or group email addresses will be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses and encouraged to use these at home for the duration of their time at CPS. Once a child leaves CPS their email account will be deleted.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

# Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems.

## User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					x
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					x
	adult material that potentially breaches the Obscene Publications Act in the UK					x
	criminally racist material in UK					x
	pornography				x	
	promotion of any kind of discrimination				x	
	promotion of racial or religious hatred				x	
	threatening behaviour, including promotion of physical violence or mental harm				x	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				x	
Using school systems to run a private business					x	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					x	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					x	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					x	
Creating or propagating computer viruses or other harmful files					x	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					x	
On-line gaming (educational)					x	
On-line gaming (non educational)					x	
On-line gambling					x	
On-line shopping / commerce			x			
File sharing					x	
Use of social networking sites			x			
Use of video broadcasting e.g. You tube, Vimeo			x			

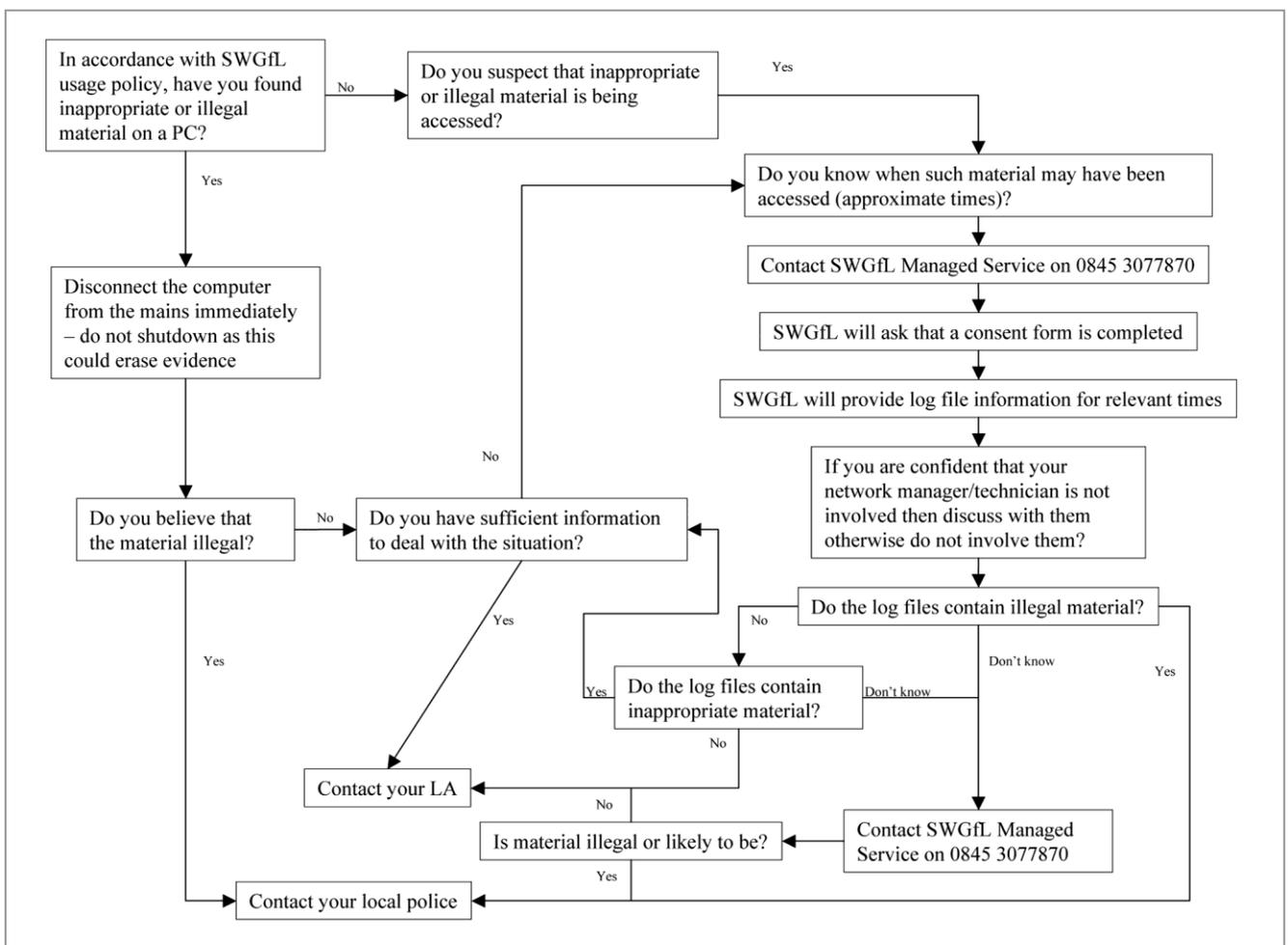
# Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

the SWGfL flow chart - below and <http://www.swgfl.org.uk/safety/default.asp> should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

## Students / Pupils

Incidents:	Refer to class teacher / tutor	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X				X		
Unauthorised use of non-educational sites during lessons	X	X						
Unauthorised use of mobile phone / digital camera / other handheld device		X			X			
Unauthorised use of social networking / instant messaging / personal email		X			X			
Unauthorised downloading or uploading of files		X						
Allowing others to access school network by sharing username and passwords		X				X		
Attempting to access or accessing the school network, using another student's / pupil's account		X					X	
Attempting to access or accessing the school network, using the account of a member of staff		X				X		
Corrupting or destroying the data of other users		X				X		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X			X		X	
Continued infringements of the above, following previous warnings or sanctions			X			X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X			X		X	X
Using proxy sites or other means to subvert the school's filtering system in order to provide educational material only		X			X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X		X				
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X			X		X	

## Constantine School Pupil Acceptable Use Policy Agreement

This Acceptable Use Policy is intended to ensure:

- that the children in our care will be responsible users and stay safe while using the school's ICT resources and the internet for all use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

### 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.

**For my own personal safety:**

- I will not use the school's ICT systems without permission.
- I will always make sure an adult is present when I am using the internet.
- I understand that the school will monitor the way I use the school's ICT systems, email and blogs.
- I will not tell anyone my password.
- I will never try to use someone else's password or user name.
- I will be aware of "stranger danger", when I am on-line.
- I will not share personal information about myself or others when on-line.
- I will never arrange to meet people off-line that I have communicated with on-line.
- I will tell an adult if I see any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable while on-line.

**I will act as I expect others to act toward me:**

- I will respect others' work and property and will not access, copy, remove or change anyone else's files, without their knowledge and permission.
- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language
- I will not take or share images of anyone without their permission.

**I understand that the school has a responsibility to make sure the school's ICT systems are secure and that they run smoothly:**

- I will not bring my mobile phone or handheld device into school unless my parent or guardian has requested this for a particular reason and I have permission from the Head Teacher to do so.
- I will not try to upload, download or access any materials which are illegal, inappropriate or may cause harm or distress to others.
- I will not try to bypass the school's filtering / security systems.
- I will tell a teacher of any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email.
- I will not install or attempt to install programs of any type on a school computer.
- I will not try to alter computer settings.
- I will never use chat and social networking sites at school. I will remember how to stay safe when using them at home.

**When using the internet I recognise that:**

- I should ensure that I have permission to use the original work of others in my own work
- I will not try to download music and video which is protected by copyright,
- I should take care to check that any information that I use is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour when I am out of school where they involve my membership of the school community.
- I understand that if I break the rules set out in this Acceptable Use Policy Agreement, I may lose access to the school's ICT systems. My parents will be informed and in the event of illegal activities, the police will be contacted.

*Please complete the section below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted access to school ICT systems.*

**I have read and understand the above and agree to follow these guidelines when:**

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, blogs, website etc.

Name of Pupil	Date
Class	
Signed (child)	Signed (parent / guardian)

## Constantine School Staff Acceptable Use Policy Agreement

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.

### Acceptable Use Policy Agreement

**For my professional and personal safety:**

- I understand that the school may 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 (email, blogs, website) 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 outlined in the e-safety policy and outside of my directed hours
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the Head teacher or ICT coordinator

**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. Where these images are published (eg on the school website / blogs) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. I understand the risks attached to using my personal email addresses / mobile phones / social networking sites for such communications.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school

- I will not use personal laptops in school
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try to upload, download or access any materials which are illegal (see e-safety policy) 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 consult the ICT coordinator before I install or attempt to install programmes of any type on a machine, or I try to alter computer settings.
- 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 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 out of school and my use of personal equipment in school 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 / or the Local Authority 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 Name

Signed

Date

### **Policy Approval History**

First approved by Full Governing Body on 11.11.2010

11.12.2012

March 2015