

## **e-Safety Policy - Development/Monitoring/Review of this Policy**

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

- School E-Safety Coordinator
- Senior Leaders
- Teachers
- Support Staff
- Governors
- Parents and Carers
- Weekly MGL firewall report monitored by IT technician

Consultation with the whole school community has taken place through the following (delete as appropriate)

- Staff meetings – various twilight sessions
- School
- Governors meeting / sub-committee meeting
- School website / newsletters

E-safety was discussed by the full Governing Body	Summer term 2017
The policy will be reviewed at the Full Governors Meeting	
The implementation of this e-safety policy will be monitored by the: Headteacher, School eSafety Coordinator	
Monitoring will take place at regular intervals:	Annually
The Governing Body / Governors Sub Committee will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Bi-annually
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:	Summer 2019
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	See diagram page

## **2. Scope of the Policy**

This policy applies to all members of the school community (staff, pupils, volunteers, parents/carers and visitors), who have access to and are users of the school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place inside and outside of school.

### 3. Context

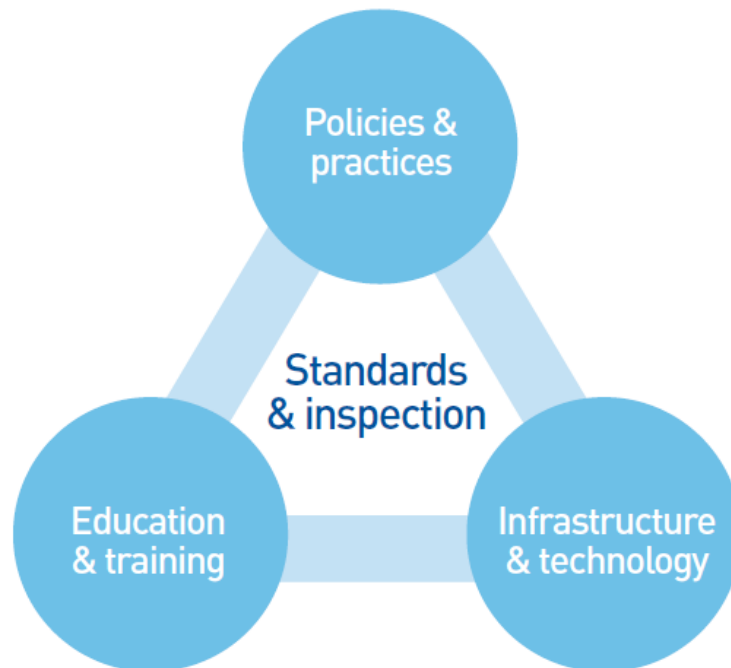
We live in a digital age where technology is playing an ever increasing part in our lives; it is changing the way that we do things both inside and outside of school and although we recognise the benefits of technology we must also be aware of the potential risks and ensure that all staff, pupils and parents/carers associated with the school are able to use technology in a safe and responsible manner.

Some of the potential dangers of using technology may 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.

Many of these risks reflect situations in the offline world but it is important that as a school we have a planned and coordinated approach to ensuring that all involved with the school use technology in a safe and responsible way. As with all risks it is impossible to eliminate them completely but with a planned and coordinated approach they can be significantly reduced and users can be taught to manage them effectively.

The school have adopted the PIES (Policy and Practice, Infrastructure, Education and Training and Standards or Inspection) model which is the basis of its approach towards E-Safety and helps to manage and minimise its risk.



### **1) Policies and practices**

The e-Safety policy outlines the importance of ICT within and outside of education. It provides guidance on the schools approach to E-Safety and details a code of conduct for school staff and pupils. The policy aims to provide an agreed, coordinated and consistent approach to E-safety. The code of conduct forms the basis of the schools expected behaviours regarding the use of technology and any infringements of the code of conduct will lead to disciplinary action against the perpetrator(s).

### **2) Infrastructure and technology**

The schools educational network and access to the internet is provided by MGL through its IT partner MGL Limited. This network provides a safe and secure 30 Mbps broadband connection to the internet via the BT data centres. There is a multi-layer security shield that provides dual-layer firewall protection, intruder detection/prevention, load balancing, content caching, data traffic analysis and virus protection. There is a client-based filtering system, Smoothwall, which filters internet content using an industry base policy. Smoothwall undertakes live scanning of all sites and blocks any threats or inappropriate websites. The infrastructure has been designed to minimise the risk of; users accessing inappropriate material, data being lost or accessed by unauthorised users, virus or malware threats. All internet and network activity is logged via the Smoothwall client system and can be retrieved if required in the event of an investigation.

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible.

### **3) Education and training**

As the use of technology and the potential risks associated with the use of the technology change rapidly, it is essential to ensure that the school community know how to use technology safely and responsibly. The school is committed to ensuring that staff receive regular training to keep up to date with new developments and ensure that they are sufficiently confident to educate pupils in the safe and responsible use of technology. The school uses the ICT Scheme 'Switched on Computing'. Within this scheme every unit has eSafety section to be taught within the plan of ICT lessons. We also use CEOP's thinkuknow website for both Key Stages to ensure pupil safety and wellbeing. The curriculum is reviewed and revised on a regular basis to ensure that it remains current. MGL are our eSafety training providers for our school, they are CEOP trained and eSafety Mark Assessors.

The school will also endeavour to provide information and training opportunities for parents and carers to raise their awareness of the technologies that their children are potential using and the risks that they potentially face.

### **4) Standards and inspection**

The school reviews its approach to E-safety on a regular basis and uses the 360° Safe tool to evaluate and improve its provision. Reference is also made to e-safety in the annual 175 audit and through Ofsted inspections.

## **4. Policy Statements**

Whilst the PIES model forms the basis of the schools approach to E-safety the school will ensure that all access to the internet and ICT systems by pupils is effectively managed and supervised.

As part of the E-safety policy the school will also manage:

- The use of digital images and video
- Data protection
- Digital communications
- Unsuitable/inappropriate activities
- Incidents of misuse

## **5. The use of digital images and video**

The development of digital imaging technologies has created significant benefits to learning, allowing school staff and pupils instant use of images they have recorded themselves or downloaded from the internet. School staff and pupils are made aware of the potential risks associated with storing, sharing and posting images on the internet and must follow the good practice detailed below.

- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they will recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are permitted to take digital images and video to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care will be taken when capturing digital images and videos that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Images and videos published on the school website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work will only be published with the permission of the pupil and parents or carers.
- Portable devices containing digital images or videos of children must not be taken off school premises.

## **6. Data Security and Protection**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

All school staff will ensure that:

- Care is taken to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Personal data is used or processed on only secure password protected computers and other devices and that these devices are properly "logged-off" at the end of any session in which they are using personal data.
- Data is transferred securely using encryption and secure password protected devices and email solutions.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
  - the data must be encrypted and password protected
  - the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
  - the device must offer approved virus and malware checking software
  - the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

## **7. Digital Communication**

Digital communication is an area that is developing rapidly with new and emerging technologies, devices are becoming more mobile and information sharing/communication is becoming more sophisticated.

When using communication technologies the school ensures the following good practice:

- The official school email service is regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, on school business or on school systems.
- Users need to be aware that email communications may be monitored
- Users must immediately report the receipt of any email 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, pupils or parents/carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Whole class or group email addresses will be used at Key Stage 1, while pupils at Key Stage 2 will be provided with individual school email addresses for educational use when appropriate and necessary.
- Pupils will 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 will not be posted on the school website and only official email addresses should be used to identify members of staff.

## **8. Unsuitable/inappropriate activities**

School ICT systems are only to be used for agreed, appropriate and suitable work related activities. Internet activity which is considered unsuitable or inappropriate will not be allowed and if discovered will lead to disciplinary action. Internet activity which is illegal will be reported and could lead to criminal prosecution.



## **9. Social Media**

### **1. Introduction**

- 1.1 Monksdown Primary School recognises its statutory responsibilities related to employment. Day to day management of staff is delegated to the Headteacher; ultimate responsibility lies with the Governing Body.
- 1.2 The Governing Body of Monksdown Primary School is committed to ensuring that all staff are aware of their responsibilities in connection with the growing use of social networking sites. It recognises that the use of such sites has become a very significant part of life for many people. They provide a positive way to keep in touch with family, friends and colleagues, and can be used to exchange ideas and thoughts on common interests. Examples of such sites include, but are not limited to, blogs (short for web logs), MySpace, Facebook, Instagram, Bebo, YouTube, Windows Live Spaces, LinkedIn, forums, bulletin boards, multiplayer online gaming, chatrooms and instant messenger apps.
- 1.3 The Governing Body will ensure that all staff are made aware of this policy and any other related ICT protocols. This policy will be easily accessible to staff and the headteacher will make any new or temporary staff aware of this policy.
- 1.4 The Governing Body expect staff to keep a professional distance from students and to make a clear separation between their private social lives and those of students. Social networking between staff and students is prohibited. The exception to this is where the school social networking sites as a communication tool with parents, the community and the wider population (see 6.1.14)
- 1.5 It is important that all staff are able to use technologies and services effectively and flexibly whilst ensuring that they do not make themselves vulnerable. The Governing Body must balance this with their duty to safeguard students and the reputation of the school and the wider community.

### **2. To whom does this policy apply?**

This policy applies to all employees, governors and volunteers at the school.

### **3. Aims:**

- to enable staff and volunteers to use social networking sites safely and securely
- to ensure staff and volunteers are aware of the risks associated with inappropriate use of social networking sites
- to safeguard staff and volunteers with respect to use of social networking sites and make sure they do not make themselves vulnerable

- to ensure the Governing Body maintains its duty to safeguard students and the reputation of the school
- to ensure duty of care towards staff and volunteers adversely affected

#### **4. Legislation**

This policy has taken account of the following legislation:

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006

#### **5. Responsibilities**

The Governing Body will:

- a) ensure this policy is implemented
- b) ensure that all staff and volunteers have access to this policy and all new employees and volunteers are made aware of it
- c) seek professional advice and support from the Human Resources provider when necessary.
- d) take appropriate action, up to and including referring the matter to the police in the case of staff and volunteers being subjected to abuse on social media.

The headteacher will:

- a) know this policy and make sure that staff and volunteers also understand the policy and their own responsibilities
- b) ensure that staff and volunteers understand the risks of the use of social networking sites and the possible implications of inappropriate use
- c) instigate disciplinary procedures where appropriate
- d) seek advice from HR providers where necessary in the case of potential misuse

Staff will:

- a) behave responsibly and professionally in connection with their use of social networking sites
- b) co-operate with the headteacher and Governing Body in implementing this policy

#### **6. Use of Social Networking Sites**

We acknowledge the right of all staff to use social media and networking to further professional knowledge and also for leisure purposes. For their own security, employees should regularly review their privacy settings on all their social networking sites; however all communication via social networking should be made with the awareness that anything said, shown or received could be made available intentionally or otherwise to an audience wider than that originally intended. If in doubt guidance should be sought from an appropriate manager. Staff are made aware of the ever greater indistinguishable line

between online and offline behaviour and are thus aware that inappropriate online behaviour has the potential to incur the same sanctions and penalties as offline misconduct.

- 6.1 Staff must not access social networking for personal use through school information systems or using school equipment
- 6.2 Staff must not accept students as friends - personal communication could be considered inappropriate and unprofessional, and makes staff vulnerable to allegations
- 6.3 In no circumstances should staff post photographs of students, except where the staff member's own children attend the school. In these circumstances, staff members may post images of their own children and friends at social events; members of staff should take care to ensure the suitability of the images and that they are not posted in relation to the school.
- 6.4 Staff are advised not to be friends with recent students; the potential for staff to be compromised in terms of wall content and open to accusations makes the risk not worth taking
- 6.5 Staff must not place inappropriate photographs on any social network
- 6.6 Staff must not post indecent remarks
- 6.7 If a member of staff receives messages via social networking that they think could be from a student, they must report it to their line manager and contact the internet service or social network so that they can investigate and take the appropriate action
- 6.8 Staff are advised not to disclose their affiliation with the school on their profile(s), or write about their work.
- 6.9 Staff must not disclose any information that is confidential to the school or disclose personal data or information about any individual which could be in breach of the Data Protection Act.
- 6.10 Staff must not disclose any information about the school that is not yet in the public arena
- 6.11 Staff must not make defamatory remarks about the school / colleagues / students / parents or post anything that could potentially bring the school into disrepute.
- 6.12 Staff should not disclose confidential information relating to their employment at the school or any member(s) of its wider community.
- 6.13 Staff should avoid language which could be deemed as offensive
- 6.14 Where a school uses social networking for communication purposes, these networks can be accessed via school equipment. School will monitor this closely and only those with administrator rights should communicate in this way. Any misuse or abuse by staff, students or the wider community should be reported to the Headteacher

## **7. Breaches of the Policy**

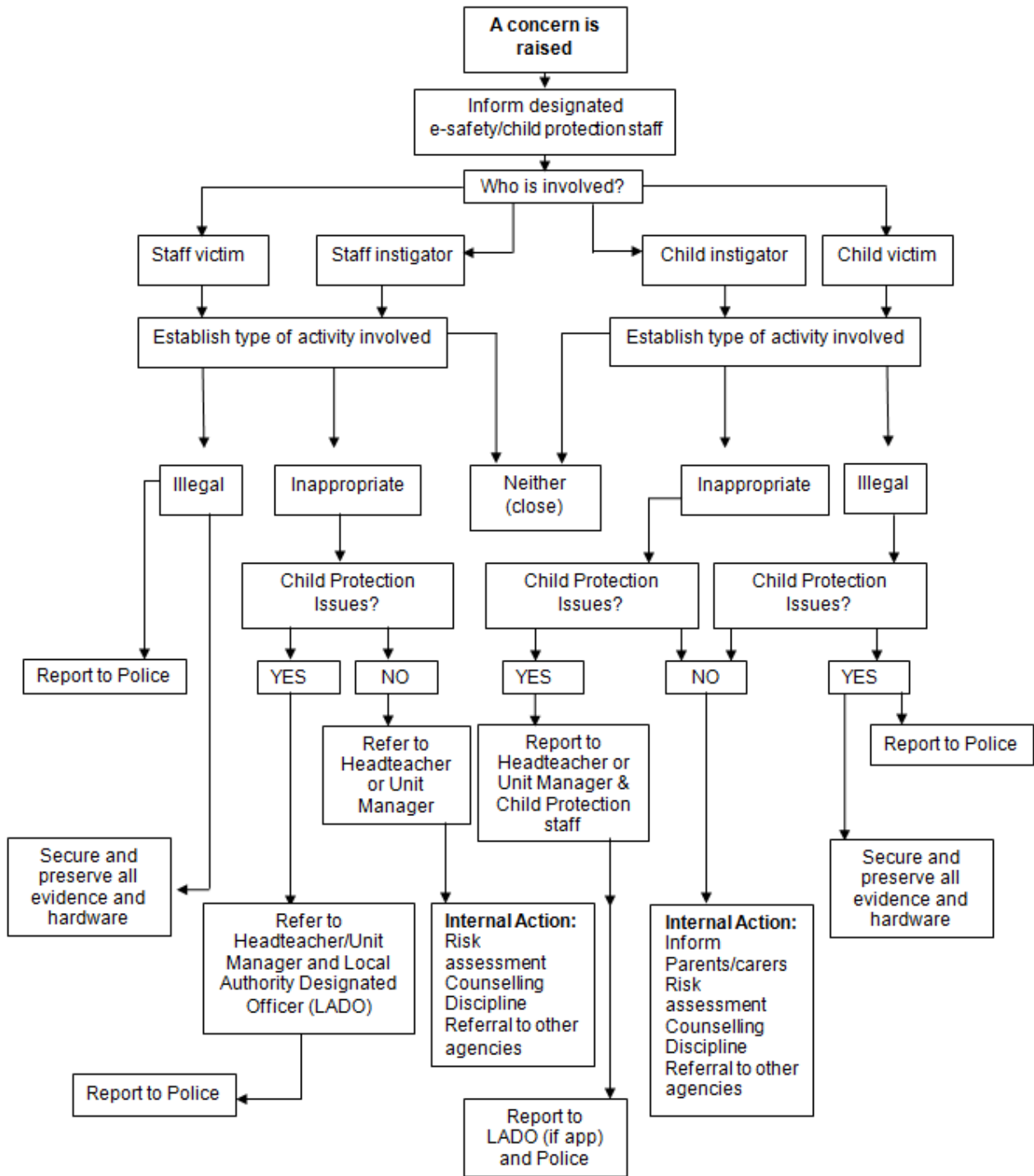
- 7.1 The Governing Body does not discourage staff from using social networking; however staff should be aware that they will take inappropriate use of social networking seriously. Any posts or comments which could be deemed online bullying or harassment will be dealt with in the same way as other instances of bullying or harassment.
- 7.2 The headteacher may take disciplinary action in the case of allegations of inappropriate use of social networking, depending on the seriousness of the allegations.
- 7.3 There may be instances where the school would be obliged to inform the police of any activity or behaviour where there are concerns about its legality
- 7.4 From time to time, staff and volunteers at school may be subject to abuse on social networking sites in connection with their role in school. Any such abuses should be reported immediately to the headteacher, who will inform governors and take whatever action is possible to deal with the situation and support the affected colleagues.

## **10. 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 accidentally, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of an e-safety incident it is important that there is a considered, coordinated and consistent approach. Incidents will be managed using the following incident flowchart.

All incidents will be recorded and reported to the relevant parties and organisations.



## Appendix A –Professional advice sheet.

### “The Nevers”

Never give personal contact details to pupils or communicate outside of school using social networks, email, text, twitter etc or meet a young person out of school unless part of a planned school activity with the knowledge of your Line Manager.

Never have conversations on social networking sites that make reference to children, parents or other colleagues at the school or be derogatory about the school.

Never make any statements or post images on social networking sites that might cause someone to question your suitability to act as a role model to young people or bring your own or the school’s reputation into disrepute.

Never communicate with parents through social network sites and you are strongly advised to declare any existing friendships/relationships to your Line Manager.

Never use personal equipment to photograph children (always use the school’s equipment) and ensure any photographs are only stored on the designated secure place on the school’s network and not on portable equipment.

Never use your personal mobile phone in areas used by children unless in emergencies or under an agreed protocol set out by the Headteacher.

**“Tech is part of life.  
Some tech is useful.  
Some of it isn’t.  
Great teachers discern”**

**Miles Berry**

paul.bradshaw@si.liverpool.gov.uk  
School Improvement Liverpool Ltd.

# Appendix B –Acceptable Use Policy

## Monksdown Primary School Acceptable Use Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

### 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.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for children's learning and will, in return, expect staff and volunteers to agree to be responsible users.

## 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 children 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 online 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, iPads, email, website, twitter 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. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- 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 / twitter) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with children and parents 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. My use of social media should be in line with the school's social media policy.

## **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:**

- When I use my mobile devices (iPads / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. Any personal mobile devices including phones should only be used in the staffroom or office and not in the presence of children unless this has been authorised by SLT.
- I will not use personal email addresses on the school ICT systems.
- 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, in accordance with relevant school policies.
- 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, nor will I try to alter computer settings, unless this is allowed in school policies



- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- 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 (schools should amend this section to provide relevant sanctions as per their behaviour policies) a warning, a suspension, referral to Governors / Directors 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 / Volunteer Name

Signed

Date