ILCHESTER COMMUNITY PRIMARY SCHOOL

e-Safety / Acceptable Use Policies (AUPs)

Date: March 2014

Review Date	Signature	Designation	Date
AUPs When Changed e-Safety March 2016			

This policy sets out the ways in which the school will:

- educate all members of the school community on their rights and responsibilities with the use of technology;
- build both an infrastructure and culture of e-Safety;
- work to empower the school community to use the Internet as an essential tool for life-long learning.

This policy is used in conjunction with other school policies.

This policy has been developed by a working group which included representatives from all groups within the school.

Scope of Policy

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

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 such as cyber-bullying, which may take place out of school, but are linked to membership of the school.

The school will manage e-Safety as described within this policy and associated behaviour and anti-bullying policies, and will inform parents and carers of known incidents of inappropriate e-Safety behaviour that take place in and out of school.

Schedule for Development, Monitoring and Review

The impact of the policy will be monitored by looking at:

- Log of reported incidents
- Internet monitoring log
- Surveys or questionnaires of learners, staff, parents and carers
- Other documents and resources
- Future developments

The e-Safety policy will be reviewed annually or more regularly in the light of significant new developments in the use of technologies, new threats to e-Safety or incidents that have taken place.

The e-Safety / AUP policy approved by
The Governing Body on ____________________________________

Signature of Chair of Governors: ____________________________________

The next review date is: ____________________________________

Roles and Responsibilities

The Headteacher is responsible for ensuring the safety (including e-Safety) of all members of the school community, though the day to day responsibility for e-Safety can be delegated.

In our school the designated Child Protection Co-ordinator will have overview of the serious child protection issues to arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate on-line contact with adults, potential or actual incidents of grooming and cyber-bullying.

Members of the Core-Curriculum team work with the e-Safety Leader to implement and monitor the e-Safety policy and AUPs (Acceptable User Policies). Views of pupils will be taken into consideration when necessary. The Core-Curriculum team meet on a termly basis.

Role	Responsibility
Governors	• Approve and review the effectiveness of the e-Safety Policy • Delegate a governor to act as e-Safety link • e-Safety Governor works with the e-Safety Leader to carry out regular monitoring and report to Governors
Headteacher and Senior Leaders	• Ensure that all staff receive suitable CPD to carry out their e-Safety roles • Create a culture where staff and learners feel able to report incidents • Ensure that there is a system in place for monitoring e-Safety • Follow correct procedure in the event of a serious e-Safety allegation being made against a member of staff or pupil • Inform the local authority about any serious e-Safety issues • Ensure that the school infrastructure/network is as safe and secure as possible • Ensure that policies and procedures approved within this policy are implemented • Use an audit[1] to review e-Safety with the school's technical support
e-Safety Leader/ Representative From the Core-Curriculum Group	• Lead the e-Safety working group • Log, manage and inform others of e-Safety incidents • Lead the establishment and review of e-Safety policies and documents • Ensure all staff are aware of the procedures outlined in policies relating to e-Safety • Provide and/or broker training and advice for staff

[1] http://bit.ly/tech_esafety_check – Document from eLIM indicating questions SLT could ask

	• Attend updates and liaise with the LA e-Safety staff and technical staff • Meet with Senior Leadership Team and e-Safety Governor to regularly discuss incidents and developments • Coordinate work with the school's designated Child Protection Coordinator

Teaching and Support Staff	• Participate in any training and awareness raising sessions • Read, understand and sign the Staff AUP • Act in accordance with the AUP and e-Safety Policy • Report any suspected misuse or problems to the e-Safety Leader • Monitor ICT activity in lessons, extracurricular and extended school activities
Pupils	• Read, understand and sign the Pupil AUP and the agreed internet rules • Participate in e-Safety activities, follow the AUP and report any suspected misuse • Understand that the e-Safety Policy covers actions out of school that are related to their membership of the school
Parents and Carers	• Endorse (by signature) the Pupil AUP • Discuss e-Safety issues with their child(ren) and monitor their home use of ICT systems (including mobile phones and games devices) and the internet • Access the school website in accordance with the relevant school AUP • Keep up to date with issues through newsletters and other opportunities • Inform the Headteacher of any e-Safety issues that relate to the school
Technical Support Provider	• Ensure the school's ICT infrastructure is as secure as possible • Ensure users may only access the school network through an enforced password protection policy for those who access children's data • Maintain and inform the Senior Leadership Team of issues relating to filtering • Keep up to date with e-Safety technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse can be reported to the e-Safety Leader for investigation

	• Ensure monitoring systems are implemented and updated • Ensure all security updates are applied (including anti-virus and Windows) • Sign an extension to the Staff AUP detailing their extra responsibilities[2]
Community Users	• Sign and follow the Guest/Staff AUP before being provided with access to school systems • Use the Online Compass tool[3] to review e-Safety

[2] http://bit.ly/elimsomersetpolicies
[3] www.onlinecompass.org.uk

Education of Pupils

A progressive planned e-Safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited.

Breadth and progression is ensured through the Somerset e-Sense progression[4] implemented through the Somerset Byte awards[5].

- Key e-Safety messages are reinforced through assemblies and Safer Internet Week (February) and throughout all lessons.

- Pupils are taught to keep themselves safe online and to be responsible in their use of different technologies as detailed in the Somerset Byte scheme of work.

- Pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material.

- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches. Staff pre-check any searches.

- Pupils are taught to be critically aware of the content they access on-line and are guided to validate the accuracy and reliability of information.

- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

- Pupils will sign an AUP for at the beginning of each school year during a class e-safety session, which will be copied to parents and carers.

Education and Information for Parents and Carers

Parents and carers will be informed about the ways the internet and technology is used in school. They have a critical role to play in supporting their children with managing e-Safety risks at home, reinforcing key messages about e-Safety and regulating their home experiences. The school supports parents and carers to do this by:

- Providing clear AUP guidance which they are asked to sign with their children and regular newsletter and web site updates;

- Raising awareness through activities planned by pupils;

- Inviting parents to attend activities such as e-Safety week, e-Safety assemblies or other meetings as appropriate.

[4] http://bit.ly/somersetesafeteaching
[5] http://bit.ly/somersetbyte

Education of Wider School Community

The school provides information about e-Safety to organisations using school facilities and local play groups and nurseries. Details about the Online Compass review tool will be shared with these groups.

Training of Staff and Governors

There is a planned programme of e-Safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the AUPs. This includes:

- An annual audit of the e-Safety training needs of **all** staff.
- **All** new staff receiving e-Safety training as part of their induction programme.
- The e-Safety Leader receiving regular updates through attendance at SWGfL and LA training sessions and by reviewing regular e-Safety newsletters from the LA.
- This e-Safety Policy and its updates being shared and discussed in staff meetings.
- The e-Safety Leader providing guidance and training as required to individuals and seeking LA support on issues.
- Staff and governors are made aware of the UK Safer Internet Centre helpline 0844 381 4772.

Cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

- The school will follow procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- The school will follow procedures to investigate incidents or allegations of cyberbullying.
- Pupils, staff and parents and carers will be advised to keep a record of the bullying as evidence.
- The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.
- Pupils, staff and parents and carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- Sanctions for those involved in cyberbullying will follow those for other bullying incidents and may include:
    - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.

- Internet access may be suspended at the school for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or AUP.

- Parent and carers of pupils will be informed.

- The police will be contacted if a criminal offence is suspected.

Technical Infrastructure

The person(s) responsible for the school's technical support will sign a technician's AUP, in addition to the staff AUP.

The school ensures, when working with our technical support provider that the following guidelines are adhered to:

- The School ICT systems are managed in ways that ensure that the school meets e-Safety technical requirements
- There are regular reviews and audits of the safety and security of school ICT systems[6].
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc from accidental or malicious attempts which might threaten the security of the school systems and data with regard to:
    - the downloading of executable files by users
    - the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices used out of school
    - the installing programs on school devices unless permission is given by the technical support provider or ICT coordinator
    - the use of removable media (e.g. memory sticks) by users on school devices. (see School Personal Data Policy for further detail)
    - the installation of up to date virus software
- Access to the school network and internet will be controlled with regard to:
    - users having clearly defined access rights to school ICT systems through group policies
    - users (apart from Foundation Stage and Key Stage One pupils) being provided with a username and password
    - users being made aware that they are responsible for the security of their username and password and must not allow other users to access the systems using their log on details
    - users must immediately report any suspicion or evidence that there has been a breach of security
    - an agreed process being in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system. All "guests" must sign the staff AUP and are made aware of this e-Safety policy
    - Key Stage 1 pupil's access to the internet will be by adult demonstration with directly supervised access to specific and approved online materials

[6] http://bit.ly/tech_esafety_check

  - Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and activities which will be adult directed

  - older pupils will apply for internet access individually by agreeing to comply with the AUP

- The internet feed will be controlled with regard to

  - the school maintaining a managed filtering service provided by an educational provider [7]

  - the school monitoring internet use

  - requests from staff for sites to be removed from the filtered list being approved by the Senior Leadership Team and logged using the Proforma provided by eLIM[8]

  - requests for the allocation of extra rights to users to by-pass the school's proxy servers being recorded, agreed and logged

  - any filtering issues being reported immediately to eLIM or SWGfL helpline

- The ICT System of the school will be monitored with regard to:

  - the school ICT technical support regularly monitoring and recording the activity of users on the school ICT systems

  - e-Safety incidents being documented and reported immediately to the e-Safety Leader who will arrange for these to be dealt with immediately in accordance with the AUP

[7] SWGfL SafetyNet

[8] http://bit.ly/somersetfiltering

Data Protection

The SWGfL Data Protection Policy[9] provides full details of the requirements that need to be met in relation to the Data Protection Act 1998.

The school will:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- use personal data only on secure password protected computers and other devices
- ensure that users are properly "logged-off" at the end of any session in which they are accessing personal data
- store or transfer data using Somerset Learning Platform (SLP), encryption and secure password protected devices from July 2014
- make sure data is deleted from the device or SLP once it has been transferred or its use is complete

Use of Digital and Video Images

Photographs and video taken within school are used to support learning experiences across the curriculum, to share learning with parents and carers on our school's learning platform and to provide information about the school on the website. The school will:

- When using digital images, instruct staff to educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.
- Allow staff to take images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.
- Make sure that images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Make sure that pupils' full names will not be used anywhere on the school website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images or videos of pupils are electronically published.
- Not publish pupils' work without their permission and the permission of their parents.
- Keep the written consent where pupils' images are used for publicity purposes, until the image is no longer in use.
- Publish a policy[10] regarding the use of photographic images of children which outlines policies and procedures.

[9] http://bit.ly/elimsomersetpolicies
[10] http://bit.ly/elimsomersetpolicies

- **Communication (including use of Social Media)**

A wide range of communications technologies have the potential to enhance learning. The school will:

- **with respect to email**
  - Ensure that all school business will use the official school email service.
  - Ensure that any digital communication between staff and pupils or parents and carers (email, chat, VLE etc) is professional in tone and content.
  - Make users aware that email communications may be monitored.
  - Inform users what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
  - If adopted provide whole class or group email addresses for use at Key Stage 1.
  - If adopted provide pupils at Key Stage 2 and above with individual school email addresses for educational use only.
  - Teach pupils about email safety issues through the scheme of work and implementation of the AUP.
  - Ensure that personal information is not sent via email.
  - Only publish official staff email addresses.
- **with respect to social media**
  - Control access to social media and social networking sites.
  - Have a process to approve staff who wish to use social media in the classroom.
  - Provide staff with the tools to risk assess sites before use and check the sites terms and conditions to ensure the site is age appropriate.
  - Make sure that staff official blogs or wikis will be password protected and run from the school website with approval from the Senior Leadership Team.
  - Inform staff not to run social network spaces for pupil use on a personal basis.
  - Publish information and share learning experiences on a school Facebook/Twitter account.
- **with respect to personal publishing**
  - Teach pupils via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
  - Advise all members of the school community not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

- Register concerns regarding pupils’ use of email, social networking, social media and personal publishing sites (in or out of school) and raise with their parents and carers, particularly when concerning pupils’ underage use of sites.

- Discuss with staff the personal use of email, social networking, social media and personal publishing sites as part of staff induction.

- Outline safe and professional behaviour.

- **with respect to mobile phones**

  - Allow staff to bring mobile phones into school but must only use them during break, lunchtimes or during non-contact when they are not in contact with pupils’ unless they have the permission of the Headteacher. They are not allowed to take photographs or video in school for any purpose without the express permission of the Senior Leadership Team.

  - Advise staff not to use their personal mobile phone to contact pupils, parents and carers.

  - Pupils should not bring mobile phones into school. All communications are directed via Office Staff.

  - Staff may carry/use a personal mobile phone during an educational trip, but will not be expected to phones pupils or parents directly. Contact will be made via Office Staff.

  - Staff should not access the school wireless network with their own personal devices without prior permission.

Assessment of risk

Methods to identify, assess and minimise risks will be reviewed regularly. As technology advances the school will examine and adjust the e-Safety Policy. Part of this consideration will include a risk assessment:

- looking at the educational benefit of the technology

- considering whether the technology has access to inappropriate material.

However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Somerset County Council can accept liability for the material accessed, or any consequences resulting from internet use.

All users need to be reminded that the use of computer systems, without permission or for inappropriate purposes, could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Police.

Reporting and Response to Incidents

The school will follow Somerset's flowcharts[11] to respond to illegal and inappropriate incidents as listed in those publications.

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The Child Protection Co-ordinator will record all reported incidents and actions taken in the School e-Safety incident log and in any other relevant areas e.g. Bullying or Child Protection log.
- The designated Child Protection Coordinator will be informed of any e-Safety incidents involving child protection concerns, which will then be escalated in accordance with school procedures.
- The school will manage e-Safety incidents in accordance with the School Behaviour Policy where appropriate.
- The school will inform parents and carers of any incidents or concerns in accordance with school procedures.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact Somerset Children Safeguarding Team and escalate the concern to the police.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Safeguarding for Schools Adviser, Local Authority Designated Officer (LADO) or Senior ICT Adviser.

If an incident or concern needs to be passed beyond the school then the concern will be escalated to the Safeguarding for Schools Adviser and eLIM 01823 356839 to communicate to other schools in Somerset. Should serious e-Safety incidents take place, the following external persons and agencies should be informed:	Safeguarding for Schools Adviser *Liz Bidmead 01823 358269 where pupil involved* Local Authority Designated Officer (LADO) *Claire Winter 01823 357823 where staff involved* Police Senior ICT adviser *Lucinda Searle 01823 356839*

The police will be informed where users 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
- promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation

[11] http://bit.ly/somersetesafetyflowcharts

- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material

Sanctions and Disciplinary Proceedings

Sanctions and disciplinary procedures may be taken where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography, adult or mature content
- promotion of any kind of discrimination, racial or religious hatred
- personal gambling or betting
- personal use of auction sites
- any site engaging in or encouraging illegal activity
- threatening behaviour, including promotion of physical violence or mental harm
- 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
- using school systems to run a private business
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and the school
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the internet

In addition the following indicates school policy on these uses of the Internet:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable
On-line gaming (educational)	✓			
On-line gaming (non-educational)		✓		
On-line gambling				✓
On-line shopping / commerce		✓		
File sharing (using p2p networks)				✓

Sanctions for Misuse: Pupils

Schools should populate the grid below marking appropriate possible sanctions.

Incidents will have unique contexts and may need different levels of sanctions especially in relation to their type and severity. Therefore ticks may appear in more than one column. The ticks in place are actions which must be followed.

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

Sanctions/Actions Staff

Schools should populate the grid below marking appropriate possible sanctions. Incidents will have unique contexts and may need different levels of sanctions especially in relation to their type and severity. Therefore marks may appear in more than one column.

The marks in place are actions which must be followed.

Incidents:	**Refer to line manager**	**Refer to Head teacher**	**Refer to Local Authority / HR**	**Refer to LADO(L)/Police(P)**	**Refer to Technical Support Staff for action re filtering etc**	**Warning**	**Suspension**	**Disciplinary action**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).				L,P				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		✓				✓		
Unauthorised downloading or uploading of files		✓				✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		✓			✓	✓		
Careless use of personal data e.g. holding or transferring data in an insecure manner		✓						
Deliberate actions to breach data protection or network security rules		✓			✓		✓	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓			✓		✓	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature staff		✓			✓		✓	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature to learners		✓	✓	L	✓		✓	✓
Breech of the school e-safety policies in relation to communication with learners		✓	✓	L			✓	✓
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils		✓	✓	L			✓	✓
Actions which could compromise the staff member's professional standing		✓	✓			✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓	✓			✓		✓
Using proxy sites or other means to subvert the school's filtering system		✓	✓			✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓	✓	L	✓	✓		✓
Deliberately accessing or trying to access offensive or pornographic material		✓	✓	L	✓		✓	✓
Breaching copyright or licensing regulations		✓	✓			✓		

Continued infringements of the above, following previous warnings or sanctions								✓

Academic Year 2013-2014

Due to this policy review taking place mid-academic year; pupil AUPs will be implemented from September 2014.

Current pupils and pupils joining up to this time will use the AUPs as outlined in the previous e-Safety Acceptable Use Policy.

APPENDIX A

Staff and Volunteer Acceptable Use Policy

School Policy

This Acceptable Use Policy reflects the school e-safety policy. The school will ensure that staff and volunteers will have good access to ICT to enable efficient and effective working, to enhance learning opportunities for pupils and will, in return, expect staff and volunteers to agree to be responsible users.

Scope of Policy

This Acceptable User Policy (AUP) policy applies to staff, volunteers and guests who have access to and are users of school ICT systems and to school related use of ICT systems outside of school.

My Responsibilities

I agree to:

- read, understand, sign and act in accordance with the School e-Safety policy;
- report any suspected misuse or concerns about e-Safety to the e-Safety Leader
- monitor ICT activity in lessons, extracurricular and extended school activities
- model the safe use ICT;
- refrain from publishing any information that: may be offensive to colleagues, may breech the integrity of the ethos of the school or may bring the school into disrepute (this includes personal sites).

Education

- I understand that I am responsible for the e-Safety education of pupils.
- I will respect copyright and educate the pupils to respect it as well.

Training

- I understand that I will participate in e-Safety training.
- I understand that it is my responsibility to request training if I identify gaps in my abilities.

Cyberbullying

- I understand that the school has a zero tolerance of bullying. In this context cyberbullying is seen as no different to other types of bullying.
- I understand that I should report any incidents of bullying in accordance with school procedures.

Technical Infrastructure

I will not try to by-pass any of the technical security measures that have been put in place by the school. These measures include:

- the proxy or firewall settings of the school network (unless I have permission);
- not having the rights to install software on a computer (unless I have permission);
- not using removable media (unless I have permission).

- **Passwords**
    - I will only use the password(s) given to me.
    - I will never log another user onto the system using my login.
- **Filtering**
    - I will not try to by-pass the filtering system used by the school.
    - If I am granted special access to sites that are normally filtered I will not leave my computer unsupervised.
    - I will report any filtering issues immediately.
- I understand that the school will monitor my use of computers and the internet.

Data Protection

- I understand my responsibilities towards the Data Protection Act and will ensure the safe keeping of personal data at all times.
- I will ensure that all data held in personal folders is regularly backed.

Use of Digital Images

I will follow the school's policy on using digital images making sure that:

- only those pupils whose parental permission has been given are published;
- I will not use full names to identify people.

Communication

I will be professional in all my communications and actions when using school ICT systems.

Email

- I will use the school provided email for all business matters.
- 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).

Social Media

- I will ask permission before I use social media with pupils or for other school related work.

Personal publishing

- I will follow the e-safety policy concerning the personal use of social media.

Mobile Phones

- I will not use my personal mobile phone during contact time with pupils.

- I will not use my personal mobile phone to contact pupils or parents.

Reporting incidents

- I will report any incidents relating to e-safety to the e-safety Leader or ICT Technician.
- I will make a note of any incidents in accordance with school procedures.
- I understand that in some cases the Police may need to be informed.

Sanctions and Disciplinary Procedures

- I understand that there are regulations in place when pupils use ICT and that there are sanctions if they do not follow the rules.
- I understand that if I misuse the School ICT systems in any way then there are disciplinary procedures that will be followed by the school.

I have read and understand the full School e-safety policy 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) in a responsible and professional manner as outlined in that document.

Staff/Volunteer Name: …………………………………………………………………………………

Signed: ………………………………………………………………………………………………**...**

Date: …………………………………………………………………………………………………

APPENDIX B

Pupil Acceptable Computer and Internet Use Policy (this AUP will be completed in class e-safety lesson, signed and copied to Parents/Carers)

Technology can help us to find information and to communicate with others.

The School encourages safe use of all technology.

All users of technology in the school must agree to certain rules and will only use the equipment and software as instructed.

My Responsibilities

I understand that I have rights and responsibilities in using ICT and will act responsibly when using technology, computers or the internet.

I will report any suspected misuse or problems to a teacher.

I will make sure there is permission to use any material that I find.

I will make sure that I maintain a healthy lifestyle do not spend too much time using technology.

Cyberbullying

I understand that the school will not accept bullying in any form.

I will be careful with all communications making sure that anything I write cannot be mistaken as bullying.

I understand that I should report any incidents of bullying.

Access to Internet Sites

I will not try to access sites that are blocked or that are unsuitable for use in school.

Communication – email, social networks, blog etc.

I will be careful in my communications making sure that nothing I write will upset others (be offensive).

I will not write anything that could be seen as insulting to the school.

Mobile Phones

Mobile phones should not be brought to school.

Sanctions

I understand that the school will monitor my use of computers and other technology.

I understand that the school may investigate incidents that happen outside school.

I understand that there are regulations in place when pupils use ICT and that there are sanctions if I do not follow the rules.

Name: ……………………………………………………………………………………...

Signed: …………………………………………………………………………………

Class: …………………………………….. **Date:** …………………………………

APPENDIX C

Pupil/Parent Acceptable Use Policy

The Internet offers both educational and social opportunities for our children. Whilst recognising the benefits we must also establish appropriate, effective and safe use of the Internet.

The Internet will be used within school to support children's learning both formally (within taught lessons) and informally (outside taught lessons), at the discretion of a member of staff who will set guidelines and rules for its use. Pupils will be taught to be critical and discriminating in their use of Internet sites and to maintain a balance between the use of technology and other activities.

Pupils may have opportunities to communicate with others through blogs, publishing work to online galleries and email. This will only take place in accordance with the school's policy and procedure, so their full name will never appear online. Responsible and considerate language will be used at all times in communicating with others.

Pupils will:

- only use the school ICT systems for those activities which they have been given permission to use and under the appropriate supervision of a member of staff.
- use the Internet within the school to support learning..
- be made aware of what cyber-bullying is and what to do if it happens.
- only use the user names and passwords they have been given
- not download and use material or copy and paste content which is copyright or not covered by the school copyright licenses.
- Not attempt to search for, view, upload or download any material that is likely to be unsuitable in a school or is blocked by the schools filter.
- inform a member of staff if they have accidentally accessed inappropriate content.
- use responsible and considerate language in communicating with others.
- be encouraged to maintain a balance between the use of ICT and other activities.
- be encouraged to discuss their use of the Internet and those sites that are age specific especially Social Network sites.
- only use mobile phones when directed by staff.
- be encouraged to talk with their parents or carers about the rules for the safe use of the Internet.
- Be made aware that the school may investigate incidents that happen outside of school but could have an effect on the school.

Failure to comply with these rules will result in one or more of the following:

- A ban, temporary or permanent, on the use of the Internet at school.
- A letter informing parents of the nature and breach of rules.
- Appropriate sanctions and restrictions placed on future access to school facilities.

If you do not understand any part of this document, you should ask a member of staff for guidance. You should only sign the Parental Permission Form when you have read, understood and have explained the importance of these rules to your son or daughter.

The form below must be completed, signed and returned to the school for our records.

Use of the Internet may be withheld unless this has been done.

I have read, understood and explained the Acceptable Use Policy to my child and I am happy for my child to experience the Internet use described:

Pupil Name (PLEASE PRINT) …………………………………………… **Class:** ……………

Name of Parent or Carer (PLEASE PRINT): ………………………………………………….

Signature: .... **Parent/Carer Date:** ……………..

APPENDIX D

Technician Acceptable Use Policy Extension

The school ICT Technician (or person given similar responsibilities) is placed in an exceptional position of trust. Many of the duties that the Headteacher expects the ICT Technician to complete are against the Staff Acceptable User Policy of the school.

This document is not a job description but an addition to the Staff Acceptable User Policy that allows the ICT technician to fulfil these duties. Schools should customise this document to fit their needs.

Areas of concern are that:

- Files may be created, imported or processed by staff and pupils and stored on the school's servers or other storage systems (e.g. USB memory sticks, SD cards etc.) that might be of an inappropriate nature to the school setting. Inappropriate use includes any production, processing or transmission of offensive, provocative, racist, unethical, irreligious or anti-social materials in any format. Also included in this area are any materials that are against the rules and conditions of service for the school e.g. material that might bring the establishment into disrepute. Work created during the school's time or on the school's equipment or on one's own equipment but for school work, belongs to the school.

- User accounts will need to be created and serviced meaning that there may be access to these accounts by the ICT technician.

- Through work within the school's administration network the ICT Technician may be placed in the position of assisting in the processing of confidential information including children's health or MIS data, confidential letters or information from or to senior staff, budgeting plans etc.

- The ICT technicians through specific user names and password have control, (sometimes through remote workstations) to the schools network. In the past there have been examples where these powers have been abused.

Because of these areas of concern the ICT Technician should:

- be responsible for monitoring the school's network.

- be given permission to access other user's files.

- protect the users by maintaining a filter for the school.

- monitor the internet use of users within the school.

- be aware of the laws relating to the use of computers especially those around Data Protection, Copyright and those referred to in the school's e-Safety Policy and AUPs.

- make sure that they record all user names and passwords for all the services they access in a place where the senior leaders in the school can access them.

- have their use of the school's network, internet and other aspects of their work open for scrutiny.

To enable them to discharge these duties they should:

- receive training on the sensitive nature of their job especially in relation to Data Protection and the confidentiality of information.
- have an agreed procedure for managing the internet filter. This should include a log of decisions made.
- have an agreed understanding of what is expected of them as far as the regular monitoring of the network system and internet.
- have agreed procedures for reporting incidents.
- log any incidents including minor ones that are quickly resolved.
- be careful to make sure that they are observed when investigating serious incidents to make sure that they are protected against any allegations that could arise (e.g. never open websites that are suspected of having inappropriate material unless others are present).
- have frequent meetings with their line manger to report on any issues or trends.

As an ICT Technician (or a person who has similar responsibilities) I have read the above document and understand that I will be directed by senior staff to complete work outside of the Staff Acceptable User Policy.

I will report all concerns I have to the appropriate member of Senior Management.

ICT Technician Name: ……………………………………………………………………………

Signed: ……………………………………………………………………………………………...

Date: ………………………………………………………………………………………………

APPENDIX E

Visitor Acceptable Use Policy

Visitors should apply certain standards when using computer equipment in schools.

These standards should include an awareness of Data Protection and Copyright laws.

Logging in

- If you use the school's equipment then request a guest log in.
- If you are using equipment that has been logged in by a member of staff always ensure a member of staff is present. Always lock the machine if they need to leave the room.
- If your service contract (Network/MIS support) allows you access to the system through team logins inform the school how you will be accessing the system.

Wireless Access

- Request permission to use the wireless connection (if available) asking for an authorisation key. You may need to change proxy settings.
- Remember that bandwidth is limited so avoid intensive use such as large downloads.

Internet Access and uploading

- The schools Internet connection is filtered so access might be denied to some sites. Seek permission to access sites that are unavailable through the schools normal filtering system. This might not be possible as changes to the filter can take some time.
- You are responsible for the sites that appear on any machine that you are using. Report any issues with the member of staff present.
- Never upload and install software or updates without permission from a member of staff.

If you use your own equipment:

- Make sure that it has up to date virus protection software installed.
- That you take care with trailing wires.
- That you can identify your equipment.
- Never leave your equipment unattended or in an unlocked room.

Downloading files or documents
For all files

- Make sure that the USB stick/external hard drive has recently been virus checked.
- Never transfer files unless you have permission.
- Make sure that you clearly state the purpose for transferring these files.
- Check to see if the school machine you would like to transfer files from or to is encrypted as it might automatically encrypt your USB stick/hard disc drive.

If the file contains sensitive personal data such as staff or student information

- Get permission for this in writing or by email.
- (Note: Where existing service contracts (Network/MIS support) indicate that this type of work will take place permission will not be needed).
- Use an encrypted memory stick or hard drive.
- Transfer the file only over a secure email connection.

If you take pictures, video or sound files then check

- That you have permission to capture these files.
- That the staff/children have all given their permission for these images/voices to be used.
- That if you intend to use these files in a public area (website, blog etc.) or for financial gain that you request this permission in writing or through email.

Name: ……………………………………………………………………………………………….

Signed: ……………………………………………………………………………………………...

Senior Member of Staff: ....

Date: …………………………………………….

APPENDIX F

Occasional Visitors e-Safety Agreement

On signing the visitors' book you agree to:

- only log onto the school network with the user name and password provided for you;
- inform the Headteacher or their representative if you intend to use the Internet, asking permission before using any kind of social media with the children;
- refrain from any use of your personal mobile phone or other device during the working day;
- not taking any photographs;
- report any suspected misuse or concerns about e-Safety whether by pupils or staff, to the Headteacher or their representative before leaving the school;
- not taking any information on pupils or staff off site unless specific permission has been given by the Headteacher or their representative;

APPENDIX G

Bring Your Own Technology (BYOT)

As new technologies continue to change the world, they also provide many new and positive educational benefits for teaching and learning. To encourage this growth we are allowing students to bring their own technology into school and use them in lessons.

This Acceptable User Policy helps educate, inform students about the use of their technology on the school site.

Definition of technology

For purposes of BYOT, technology means any privately owned portable equipment such as laptops, ultra books, smart phones, cameras, any device capable of accessing the internet etc.

Internet

Only the internet connection provided by the school may be accessed while on the school site. Accessing the internet through a signal that does not go through the filtered access provided by the school is not allowed at any time.

Security and Damages

Responsibility to keep the device secure rests with the individual owner. The school, nor its staff or employees, are liable for any device stolen or damaged on the school site. If a device is stolen or damaged, it will be handled through the school policies similar to other personal belongings. It is recommended that decals, other custom touches and UV markings are used to physically identify the device. Protective cases should be used as well. If the device is capable of being GPS tracked then this should also be activated.

BYOT Student Agreement

The use of technology to provide educational material is not a necessity but a privilege. A student does not have the right to use his or her laptop, mobile phone or other electronic device while at the school. When abused, privileges will be taken away.

Students and parents or guardians partaking in BYOT must adhere to the student code of conduct, as well as all other school policies, particularly the e-safety policy and the associated Student Acceptable User policy.

Additionally, technology:

- Must be in silent mode on the school site and on school buses
- May not be used in tests or exams
- Must only be used to access files or computer or internet sites which are relevant to the curriculum. Games are not permitted

Students acknowledge that:

- The schools network filters will be applied to the internet connection and attempts will not be made to bypass them
- Their personal device is virus protected and is not capable of passing on infections to the schools network

- Hacking, damaging or by passing the school internet security procedures is against the school policies
- The school has the right to collect and examine any device that is suspected of causing problems, either technical or from abuse of other school policies
- Printing from personal laptop devices will not be possible
- Personal technology is charged prior to bringing it to school and runs off its own battery. Charging will not be possible during the school day

Please read and sign the BYOT agreement. No student will be allowed personal technology devices unless the agreement is signed and returned. Students, parents and guardians participating in BYOT, must adhere to all school policies.

Please read carefully and initial every statement

	Students take full responsibility for their devices. The school is not responsible for the security of personal technology. Personal devices cannot be left on school property before or after school hour.
	Devices cannot be used during tests or exams.
	Student must immediately comply with the teachers request to shut down or close devices. Devices must be in silent mode and put away when asked by teachers.
	Personal devices must be charged prior to bringing them to school and run off their own batteries while at school.
	To ensure appropriate network filters, students will only use the school internet connection and will not attempt to by-pass this
	Students must make sure that their device is virus protected and is not capable of infecting the school network.
	Students realise that printing for personal devices will not be possible.
	Students should not share their device with other students, unless they have written permission to do so.
	The school retain the right to confiscate and examine any device.
	The school will inform parents or guardians of any misuse and in some cases, if confiscated, only return the device to the parent or guardian.

Please understand that the use of personal devices to support educational experience is not a necessity but a privilege. With respect of the rules, this privilege will benefit the learning environment as a whole. When rules are abused privileges will be taken away.

I understand and will abide by the above policy and guidelines. I further understand that any violation is unethical and may result in the loss of my technological privileges as well as other disciplinary action.

Name: ……………………………………………………………………………………………..

Signature: ……………………………………………………**Student** **Date:** …………….

Signature: ……………………………………………**Parent/Carer** **Date:** …………….