South Gloucestershire Council

St Chad's Patchway CE VC Primary School

'Learning to love, loving to learn'

COMPUTING ACCEPTABLE USE POLICY

INTRODUCTION

Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of Computing within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

At St. Chad's Patchway CE VC Primary School, we understand the responsibility to educate our pupils on E-Safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

SCOPE OF THE POLICY

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school computer systems, both in and out of the 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 outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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 out of school.

ROLES AND RESPONSIBILITIES

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school

Governors:

Governors are responsible for the approval of the E-Safety Policy 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.

Headteacher and Senior Leaders:

- The Headteacher has a duty of care 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 should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (See flow chart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR disciplinary procedures).

E-Safety Coordinator / Officer:

- 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;
- liaises with school technical staff

- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments/

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 / academy* e-safety policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP).
- They report any suspected misuse or problem to the Headteacher and/or E-Safety Coordinator *for* investigation / action / sanction.
- All digital communications with students / pupils / parents / carers should be on a professional level.
- Students / pupils understand and follow the e-safety and acceptable use policies
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection Officer

Should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Pupils:

- are responsible for using the school's digital technology systems in accordance with the Pupil Acceptable Use Policy;
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- 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 / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature.

Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events;
- Access to parents' sections of the website and on-line student / pupil records;

EDUCATION: PUPILS

Online safety is now a statutory part of the programme of study for all key stages. Rules and technical solutions are not infallible and we are aware that outside school children will be using unfiltered internet provision. We believe it is crucial to educate children about how to behave responsibly online and how to keep themselves and others safe.

Children and young people need the help and support of the school and parents to recognise and avoid e-safety risks. There is a planned and progressive scheme of work for online safety which is taught at every year group. This is based around the Digital Literacy Curriculum by SWGfL and, across the key stages, covers strands on:

- Internet safety
- Privacy and security
- Relationships and communication
- Cyberbullying
- Information literacy
- Self-image and identity
- Digital footprint and reputation
- Creative credit and copyright

Rules for Keeping Safe

These are reinforced through the following:

- Pupils sign an acceptable use agreement and this is also communicated to parents who we hope will reinforce the messages at home.
- Pupils are helped to understand the student acceptable use policy and school rules for online safety and encouraged to act accordingly.
- Staff act as good role models in their own use of computers.
- Staff are aware that there may be some children that are more vulnerable than others to being approached online and endeavour to ensure that these children understand the issues involved.
- Online behaviour is dealt with in accordance with our behaviour policy. There are sanctions and rewards in place for this.

Self-evaluation and Improvement

The school undertakes self-evaluation in order to inform actions to improve e-safety provision through the following:

- Local authority safeguarding audit
- 360 degree safe online self-evaluation tool which is also used to benchmark our provision against other schools.
- Surveys with pupils and staff

EDUCATION – PARENTS / CARERS

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children’s on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities;
- Letters, newsletters, web site;
- Parents / Carers evenings / sessions;

- High profile events / campaigns e.g. Safer Internet Day;
- Reference to the relevant web sites / publications

EDUCATION & TRAINING – STAFF / VOLUNTEERS

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows: (select / delete as appropriate)

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All 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 Agreements.
- The E-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days as necessary
- The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

TRAINING – GOVERNORS

Governors should be invited to take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation;
- Participation in school training / information sessions for staff or parents.

TECHNICAL ISSUES

The local authority provides technical and curriculum guidance for e-safety issues for all South Gloucestershire schools.

Password Access to Systems

All our systems are accessed via an individual log in. Users have passwords that include upper and lower case and a number and are encouraged to change these regularly. Users are told that passwords must never be shared for any IT system and that they are responsible for any actions taking using their log in.

Internet Provider and Filtering

The South Gloucestershire school internet service is provided by Traded Services and this includes a filtering service to limit access to unacceptable material for all users. Illegal content (child sexual abuse images) is filtered by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. However we are aware that no filtering is completely infallible and consequently focus on teaching pupils to keep safe through our curriculum and teaching. There are two different levels of filtering which are targeted towards different user groups. As a consequence teacher and staff users have access to some resources for teaching that are filtered for learners.

Requests from staff for sites to be removed from the filtered list must be approved by the head teacher and this is logged and documented by a process that is agreed by the Headteacher. Any filtering requests for change and issues are reported immediately to the South Gloucestershire technical team on 3838.

Proactive monitoring is in place via a monitoring box provided by SWGfL. Should anyone attempt to access illegal content this is immediately reported to the police. Illegal activity would include attempting to access:

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Technical Staff - Roles and Responsibilities

Where the local authority provides technical support the "administrator" passwords for the school are not held by the school and the local authority are responsible for their security and any implications of their use. The school ensures, when working with our technical support provider that the following guidelines are adhered to.

- There are regular reviews and audits of the safety and security of school computer systems.
- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All users have clearly defined access rights to school computer systems and are provided with a username and password by the technical support provider.
- Users are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- An agreed policy is in place (to be described) for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- School computer technical staff regularly monitor and record the activity of users on the school computer systems and users are made aware of this in the Acceptable Use Policy.
- 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.
- The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place (to be described) regarding the downloading of executable files by users
- An agreed policy is in place (to be described) regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy is in place that forbids staff from installing programmes on school workstations / portable devices.
- An agreed policy is detailed regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices in our acceptable use agreement.

USE OF DIGITAL AND VIDEO IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet,

- In accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images 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 should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the 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 students / pupils are published on the school website

Communications Technologies and Social Media

A wide range of communications technologies have the potential to enhance learning and management. The acceptable use agreements outline how these systems should be used.

- The official school email service is used for communications between staff, and with parents/carers and students, as it provides an effective audit trail.
- Users are made aware that email communications may be monitored and what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature through the acceptable use policies.
- Personal email addresses, text messaging, public chat and social networking programmes are not be used for communications with parents/carers and children.
- An online secure platform is used for pupil learning and this includes secure access to communications tools so that children can learn about these within a limited environment.
- Personal information is also not posted on the school website and only official email addresses are listed for members of staff.
- Guidance on personal use of social media and mobile devices is included in the staff, parent and pupil acceptable use policies.

DATA PROTECTION

Personal data will be recorded, processed, transferred and made available according to the GDPR 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.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section in the appendix)
- It has a Data Protection Policy (see appendix for template policy)
- It is registered as a Data Controller for the purposes of the GDPR.
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- 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, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory 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

REPORTING AND RECORDING

There are clear reporting mechanisms in place for online safety incidents and all staff are regularly reminded of these and fully aware of their responsibilities to follow up any reported issues.

- Online safety issues are reported to the Online Safety Lead. If these include allegations of bullying then the anti-bullying policy is followed.
- Issues which may impact on the well-being and safety of a child are reported directly to the Child Protection Lead and Child Protection procedures are followed.
- Staff who are targeted by bullying online report these issues to the head teacher.
- Any member of staff seeing something online that is negative about the school reports this to the head teacher.

- Pupils are encouraged to report any incidents to an adult whether it relates to themselves or a friend. We encourage children to take responsibility for protecting each other.
- Younger pupils are shown how to use Hector Protector if they access unsafe content and older pupils are also shown how to report online in case of incidents outside school.
- If issues could be a result of problems with infrastructure or may affect it then the technical support provider is informed immediately (for South Gloucestershire support 3838).
- If access to an unsuitable site is reported then the Online Safety lead will alert the technical support team by ringing 3838 to ensure that this is blocked.
- Serious incidents are escalated to local authority staff for advice and guidance
    - Nick Pearce – Infrastructure, Technical and Filtering - 3838
    - Jo Briscombe – Curriculum and Policy – 3349
    - Leigh Zywek – Safeguarding and Child Protection - 5933
    - For incidents affecting school staff the Professionals Online Safety Helpline is contacted for advice if necessary on helpline@saferinternet.org.uk or 0844 381 4772.

Any reported incidents are logged in the online safety log and followed up in accordance with the relevant policy depending on the issue. The response is also logged and serious issues are followed up after an interval of time to ensure that they are fully resolved.

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. The school policy restricts usage as follows:

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	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X

contain or relate to:	**criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986**					X
	pornography				X	
	promotion of any kind of discrimination				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	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					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	
Unfair usage (downloading / uploading large files that 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 media				X		
Use of messaging apps				X		
Use of video broadcasting e.g. YouTube					X	

SCHOOL ACTIONS & SANCTIONS

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 **Actions / Sanctions**

Incidents:	Refer to class teacher	Refer to Head of Key Stage/ E-Safety Co-ordinator	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).		X	X	X					
Unauthorised use of non-educational sites during lessons	X	X						X	X
Unauthorised use of mobile phone / digital camera / other mobile device	X	X				X		X	X
Unauthorised use of social media / messaging apps / personal email	X	X			X			X	X
Unauthorised downloading or uploading of files	X	X	X		X	X		X	X
Allowing others to access school network by sharing username and passwords		X	X		X			X	X
Attempting to access or accessing the school network, using another pupil's account	X	X						X	X
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X			X	X	X	X
Corrupting or destroying the data of other users	X	X	X			X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X	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	X	X	X

Using proxy sites or other means to subvert the school’s / academy’s filtering system	X	X	X			X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X			X		X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	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			X	X	X	X

Staff **Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority	Refer to Police	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).		X	X	X				
Inappropriate personal use of the internet / social media / personal email		X				X		
Unauthorised downloading or uploading of files						X		
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						X		
Careless use of personal data e.g. holding or transferring data in an insecure manner						X		

Deliberate actions to breach data protection or network security rules	X	X				X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X				X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X				X		X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X			X		X
Actions which could compromise the staff member's professional standing						X		
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy						X		
Using proxy sites or other means to subvert the school's / academy's filtering system	X	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
Breaching copyright or licensing regulations						X		
Continued infringements of the above, following previous warnings or sanctions								X

ROLES AND RESPONSIBILITIES

Role	Responsibility
Governors	Approve and review the effectiveness of the E-Safety Policy and acceptable use policies E-Safety Governor works with the E-Safety Leader to carry out regular monitoring of e-safety incident logs, filtering, changes to filtering and then reports to Governors

Head teacher and Senior Leaders:	Ensure that all staff receive suitable CPD to carry out their e-safety roles and sufficient resource is allocated. 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 Inform the local authority about any serious e-safety issues including filtering Ensure that the school infrastructure / network is safe and secure and that policies and procedures approved within this policy are implemented.
E-Safety Leader:	Lead the e-safety working group and dealing with day to day e-safety issues Lead role in establishing / reviewing e-safety policies / documents, Ensure all staff are aware of the procedures outlined in policies Provide and/or brokering training and advice for staff, Attend updates and liaising with the LA e-safety staff and technical staff, Deal with and log e-safety incidents including changes to filtering, Meet with E-Safety Governor to regularly to discuss incidents and review the log Report regularly to Senior Leadership Team
Curriculum Leaders	Ensure e-safety is reflected in teaching programmes where relevant e.g. anti bullying, English publishing and copyright and is reflected in relevant policies.
Teaching and Support Staff	Participate in any training and awareness raising sessions Have read, understood and signed the Staff Acceptable Use Agreement (AUP) Act in accordance with the AUP and e-safety policy Report any suspected misuse or problem to the E-Safety Co-ordinator Act professionally and safely when using technology Monitor computing activity in lessons, extra-curricular and extended school activities Deliver the scheme of work for online safety Use opportunities in the curriculum to reinforce online safety messages
Students / pupils	Participate in e-safety activities, follow the acceptable use policy 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 Student / Pupil Acceptable Use Policy Ensure that their child / children follow acceptable use rules at home Discuss e-safety issues with their child / children and monitor their home use of computer systems (including mobile phones and games devices) and the internet Access the school website / Merlin in accordance with the relevant school Acceptable Use Policy. Keep up to date with issues through school updates and attendance at events
Technical Support Provider	Ensure the school's computer infrastructure is secure in accordance with Becta guidelines and is not open to misuse or malicious attack Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly changed for those who access children's data Inform the head teacher of issues relating to the filtering applied by the Grid 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 / attempted misuse can be reported to the E-Safety Co-ordinator for investigation / action / sanction. Ensure monitoring software / systems are implemented and updated Ensure all security updates / patches are applied (including up to date anti-virus definitions, windows updates) and that reasonable attempts are made to prevent spyware and malware.
Community Users	Sign and follow the AUP before being provided with access to school systems.

MONITORING AND EVALUATION

The school will review this policy every two years and assess its implementation and effectiveness. The policy will be promoted and implemented throughout the school and all members of staff will be given a copy.

Signed …………………………………. Chair of governors Date…………

Signed…………………………………. Headteacher Date………