St Michael's Primary School
E-safety policy (includes ICT security)

Policy ratified by the *Governing Body on:*	Monday 15th January 2018 Amended February 2021
The implementation of this policy will be monitored by:	Curriculum and Achievement Committee
This policy will be reviewed:	Every 4 years, or sooner as needed
Should serious Online safety incidents take place, the following external persons / agencies will be informed:	Nick Pearce – Technical and Filtering Jo Briscombe – Teaching and Leaning Adviser ICT

Monitoring

The school will monitor the impact of the policy through an analysis of:

- Logs of reported incidents and responses
- Network monitoring data
- Surveys / questionnaires of students, parents / carers, and staff including non-teaching staff
- Monitoring information about the teaching programme and coverage within the curriculum
- Regularly checking that pupils and staff are clear about how to report incidents and respond to them
- The content of the web site is regularly monitored by the Headteacher to ensure that it complies with this policy and the acceptable use policies.
- Any other platforms, such as class dojo and tapestry, will also be regularly monitored to ensure that the school is always presented accurately and professionally.

Scope of the Policy

This policy applies to **all** members of the school community (including volunteers, parents/carers, visitors and community users) who have access to or use school ICT systems inside and outside school. The Education and Inspections Act 2006 empowers Head teachers, 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 relevant to incidents, including cyber-bullying, which may take place out of school, but are 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, inform parents / carers of known incidents of inappropriate Online safety behaviour that take place out of school. The 2011 Education Act increased these powers with regard to searching for and of electronic devices and the deletion of data and related action can only be taken over issues covered by the school behaviour policy. When dealing with online safety issues, electronic devices will only be searched and data deleted with parents. If parents are unavailable the device will be kept securely until a parent can meet to conduct such a search with a senior leader.
This policy should be read alongside the acceptable use policies for staff and pupils, the anti-bullying policy and the behaviour policy.

Roles and Responsibilities

These are clearly detailed in Appendix 1 for all members of the school community.

- The governors have overall responsibility for ratifying the policy, ensuring that it is implemented and monitoring it. This action is delegated to the Curriculum Committee.
- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety is delegated to the online safety Leader, Chris Keating.
- The head teacher is also the designated person for child protection and is trained in online safety issues and aware of the potential for serious child protection 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 and cyber-bullying.

Teaching and Learning
Online safety is now a statutory part of the programme of study for all key stages. Rules and technical solutions are 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 online 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 South Gloucestershire scheme of work and Digital Literacy Curriculum by SWGfL and, across the key stages, covers:

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

The scheme of work is delivered as part of computing, PSHE and across our creative curriculum. Regular opportunities are taken to reinforce online safety messages in all lessons and to teach pupils to be critically aware and consider the accuracy of the information they access online. Online safety messages are also reinforced through other subjects and through a planned programme of other activities such as assemblies and events. Older pupils are taught to acknowledge the source of information and respect copyright. Pupils are helped to understand the ~~AUP~~Acceptable Use Policy (AUP), recognise online safety risks, adopt safe practices, report any issues and keep evidence to support reporting (for older children). Staff model safe practice in use of technologies and mobile devices and guide students to appropriate sites and follow practices for dealing with unsuitable material found in internet searches. Where pupils undertake searching of the internet staff monitor the content of the websites they are visiting. If they identify pupils who may be vulnerable, for example, who are not adopting safe practices or completing inappropriate searches this should be logged and appropriate support given to those pupils to help them understand the risks and what to do to keep safe.
If there are educational reasons why a blocked site is needed for learning then staff can request that this be made available to technical staff. Where this is done this is clearly logged with reasons given for this access.
Annual online safety events such as Safer Internet Day are also used to raise awareness.

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.
- All classes have online safety rules displayed in their classroom and staff regularly refer to these, for example, during activities where children are searching the internet for information.
- Staff act as good role models in their own use of ICT.
- 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.

Education – parents / carers and the community
Parents and carers have an essential role in educating their children and monitoring their behaviour online, however they may have a limited understanding of the risks and issues and underestimate the dangers or be unsure how to deal with them. The school aims to raise awareness and support parents through:

- Curriculum activities
- Letters and newsletters including information on any online safety issues that have been raised in school (anonymously recorded) and how to address these

- Parents / carers information evenings
- Events such as Safer Internet Day
- Providing information and weblinks about where to access support on the website
- Parents of children who join school mid-year are made aware of the processes and their children are also introduced to the acceptable use policy (AUP) depending on their age.

Education – staff and volunteers
All staff receive regular online safety training so that they understand the risks and their responsibilities. This includes:

- A planned programme of online safety training which is regularly updated and reinforced and linked to the expectations outlined in this policy, Keeping Children Safe in Education and in the Ofsted framework.
- An audit of online safety training needs of staff is carried out ~~regularly.~~periodiacally
- All new staff receive online safety training and training on relevant policies and expectations as part of their induction programme.
- The headteacher receives regular updates ~~and external training~~ to support them to do their role.
- Policies relevant to online safety and their updates are discussed in staff meetings.
- The headteacher and e-safety coordinator provide~~s~~ regular guidance and training to support individuals where required.

Training – governors
Governors take part in online safety training and awareness raising sessions, particularly those governors who are involved with technology and safeguarding. This is offered through:

- Attendance at local authority or regional events
- Attendance at relevant staff training
- Regular newsletter information and access to website information

Self-evaluation and Improvement
The school undertakes self-evaluation in order to inform actions to continually improve online safety provision through the following:

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

Technical Issues
The local authority provides technical and curriculum guidance for Online safety issues for South Gloucestershire schools as well as providing direct technical support to a large number of schools.

Password Access to Systems
All our systems are accessed via an individual log-in. Passwords must never be shared for any IT system and users are responsible for any actions taken using their log-in. All higher-level systems (eg ~~SIMS~~Arbor, CPOMS) have additional log-ins and separate passwords.

Internet Provider and Filtering
The ~~South Gloucestershire~~ school's internet service is provided by ~~Integra~~ Soltech, our IT support partner . This~~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 so as to ensure that "over blocking" does not restrict teaching.

- Technical staff monitor internet traffic and report any issues to schools.
- The school reports issues through logging a call to ~~the service desk at 3838.~~Soltech.
- Any filtering requests for change and issues are also reported immediately ~~to the South Gloucestershire technical team on 3838.~~ Soltech. 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.~~

Technical Staff - Roles and Responsibilities

~~The LA supports admin ICT and Apollo supports curriculum ICT.~~All IT systems are support by Soltech – admin and curriculum.

~~In both cases the~~The "administrator" passwords for the school are ~~not held by the school and the local authority/Apollo are responsible for their security and any implications of their use.~~held by Soltech.

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

- There are regular reviews and audits of the safety and security of school I~~C~~T systems.
- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All users have clearly defined access rights to school I~~C~~T 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.
- Temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system must be authorised by the Headteacher or School Business Manager.
- 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.
- Only the technicians have permissions to install executable files or programmes.
- Any school device (e.g. laptops) can be used off the school premises, but should only be used by the member of staff themselves.
- Any removable media containing confidential information must be password protected.

Use of Digital Images and Video

Ease of access to technologies which take digital images and video has many benefits for learning. Taking and sharing images and video, if not managed, could increase the risk of misuse and has the potential to be used for cyberbullying. The school informs and educates users about the risks associated with digital images and these are outlined in the acceptable use policies:

- When using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including publishing their own images on social networking sites.
- Pupils should not take, use, share, publish or distribute images / video of others without their permission and staff reinforce this when appropriate.
- Written permission is obtained from parents or carers before photographs of pupils are taken. These photographs are only taken to be used for educational purposes or to promote achievements or the school.
- Staff are allowed to take digital / video images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.
- Staff sign permission forms to say that they allow their image to be used for promoting the school and are aware of the risks of this being copied
- Images are only taken and used of individuals where there is a signed permission form in place.
- Pupils' full names are not published on any online platform or school communication including the web site, newsletter or other media. Photographs published anywhere that include pupils are carefully selected and not used in association with pupils' full names or other information that could identify them.
- Care is always taken to ensure that pupils are appropriately dressed if images are taken and that they are not participating in any activity which might bring individuals or the school into disrepute.
- 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 this is not covered by the Data Protection Act. However in order to protect other children and respect privacy these images should not be published or made publicly available on social networking sites. Parents / carers should also not comment on any activities involving

other pupils in the digital / video images. This is clearly detailed in our acceptable use policy for parents.
- Pupils' work is only published with the permission of pupils and parents / carers.

Mobile Technologies
These might include mobile phones, tablets or any other device that has the capability of accessing the school's wireless network. The primary use of these in school is to support learning, teaching and management.
Children are not allowed to use their personal devices in school as the school provides access to the technologies to be used for learning. If children bring devices into school for use before/after school they must first secure permission from the school using the appropriate for. Devices must be given to the teacher at the start of the school day, and held securely throughout the day.
Staff are not allowed to use their personal mobile phones in school while they are teaching and any use should be restricted to times when children are not present. The only exception to this is in case of emergency during a school trip.
Staff should ~~not use~~avoid using their own mobile phone to take images of children, for example, on a school trip but should use a school device, eg ipad. Any images taken on a phone should be downloaded to the school system as quickly as possible and then deleted from the device.~~one of the school cameras.~~

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. Communications are always professional in tone and content.
- 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.
- Governor communications should take place through governor school e-mail accounts. Personal or sensitive information is not e-mailed but is kept on a secure drive on the school computer system.
- Personal email addresses, text messaging, public chat and social networking programmes are not be used for communications with parents/carers and children.
- Where the school uses apps such as the website app, Twitter etc, these are managed and monitored by a named member of staff who approves content and monitors use of the account.
- Personal information is also not posted on the school website and only official email addresses are listed for members of staff. The web site is under ~~the~~ the responsibility of the Headteacher.
- Guidance on personal use of social media and mobile devices is included in the staff, parent and pupil acceptable use policies including clear reporting mechanisms. Training is provided for staff and risks, reporting and issues around social networking forms part of the learning for pupils.
- Staff ensure that no reference is made in social media to pupils, parents or other staff and do not engage in online discussions on personal matters about any member of the school community
- Staff personal use of social media where it does not relate to the school is outside the scope of the policy but is should be made clear that the member of staff is not communicating on behalf of the school. If staff come across communications that might bring the school into disrepute in their personal communications they should not get involved, refer the publisher to relevant complaints procedures and report the issue.

Copyright
The Headteacher is responsible for making sure that software licence audit is regularly updated and also making regular checks to ensure the number of software installations matches the licences held. Where there are insufficient licences this could breach the Copyright Act which may lead to fines or unexpected additional license costs.

Data Protection
Personal Data is defined as any data which relate to a living individual who can be identified from the data. This includes opinion about the individual. Sensitive Personal Data about a person includes information about their racial or ethnic origin, political opinions, their religious beliefs or other beliefs of a

similar nature, whether they are a member of a trade union and their physical or mental health or condition. Actions are currently being implemented in order to ensure compliance with ~~the~~the ~~new~~current GDPR (Government Data Protection Regulation) and this policy will be updated in line with this new legislation.

Personal data is recorded, processed, transferred and made available according to the General Data Protection Regulation 2018 and is:

- 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 and only transferred to others with adequate protection

Transfer of Data

Whenever possible secure online storage is used to ensure that documents do not need to be transferred to limit the risk. We ensure that data is stored in accordance with the requirements laid down by the Information Commissioner's Office. ~~and within the EU.~~ This also applies to cloud storage used.

The school ensures that:

- It holds the minimum personal data necessary to enable it to perform its function and does not hold it for longer than necessary for the purposes it was collected for.
- The data held is accurate, up to date and inaccuracies are corrected as quickly as possible.
- All personal data is fairly obtained in accordance with our "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing" as outlined in the policy on the South Gloucestershire IMS Traded Services web site.
- Personal and sensitive data relating to pupils or staff is not e-mailed as this is not secure.
- Personal data including assessment data is transferred using secure file transfer.
- Where information does need to be transferred between devices then encrypted memory sticks are used.
- It has clear and understood arrangements for the security, storage and transfer of personal data
- It is registered as a Data Controller for the purposes of the GDPR.
- Integra is currently contracted as the~~We are in the process of putting a~~ Senior Information Risk Officer (SIRO) and Information Asset Owner (IAOs). ~~in place.~~
- Risk assessments are regularly carried out.
- Data subjects have a right to access their data and there are clear procedures for this.
- 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.
- Only cloud storage that meets the requirements laid down by the Information Commissioner's office is used to store personal data.
- The staff acceptable use policy clearly defines the data protection measures that staff should take and how data can be securely stored and deleted.

Staff ensure that they

- Take care to ensure safe keeping of personal data and minimise the risk or loss or misuse
- Use personal data only on secure password protected computers and devices and log off at the end of every session
- Transfer data using encryption and secure password protected devices

Where personal data is stored on removable media:

- ~~The~~ Personal data is encrypted and password protected
- The device is password protected
- The device has approved virus and malware checking software
- The data is securely deleted from the device once finished with.

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.

Staff should report online safety issues are reported to the headteacher. 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. Issues impacting on staff or to the detriment of the school should be reported to the headteacher or to the Chair of Governors if the headteacher is absent or the accusation involves the headteacher.
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.

Managing Incidents
In the event of suspicion of an infringement of policy then all the following steps should happen.

- More than one senior member of staff should be involved in investigating to protect possible future accusations.
- Use a computer that will not be used by young people which could be taken off site by the police if required.
- Ensure staff have internet access to investigate but that sites and content are closely monitored and recorded.
- Record the URL of any site containing alleged misuse and the nature of the content causing concern. It may be useful to record and store screenshots of the content by printing them, signing them and attaching them to the record. Not with child abuse images.
- Once the investigation is complete the investigating group should identify the appropriate response in line with policies which may internal procedures, involvement of LA or police.

Reporting to the police

- If the content being reviewed includes images of child abuse then monitoring should be stopped and the police informed immediately. Other incidents to be referred to the police are
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials

  In any of the above isolate the computer involved as any change to its stage may hamper a police investigation.

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~~at Soltech 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
Tina Wilson – Safeguarding and Child Protection - 8508

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.

Where appropriate school newsletters and the website are used to provide guidance to staff following an incident in order to prevent further incidents happening.

There are defined sanctions in place for any breaches of the acceptable use policies. Suggestions for these can be accessed in SWGfL policy template (Word version with appendices) on pages 17 – 19.

This policy will be reviewed every 4 years, or sooner as needed.

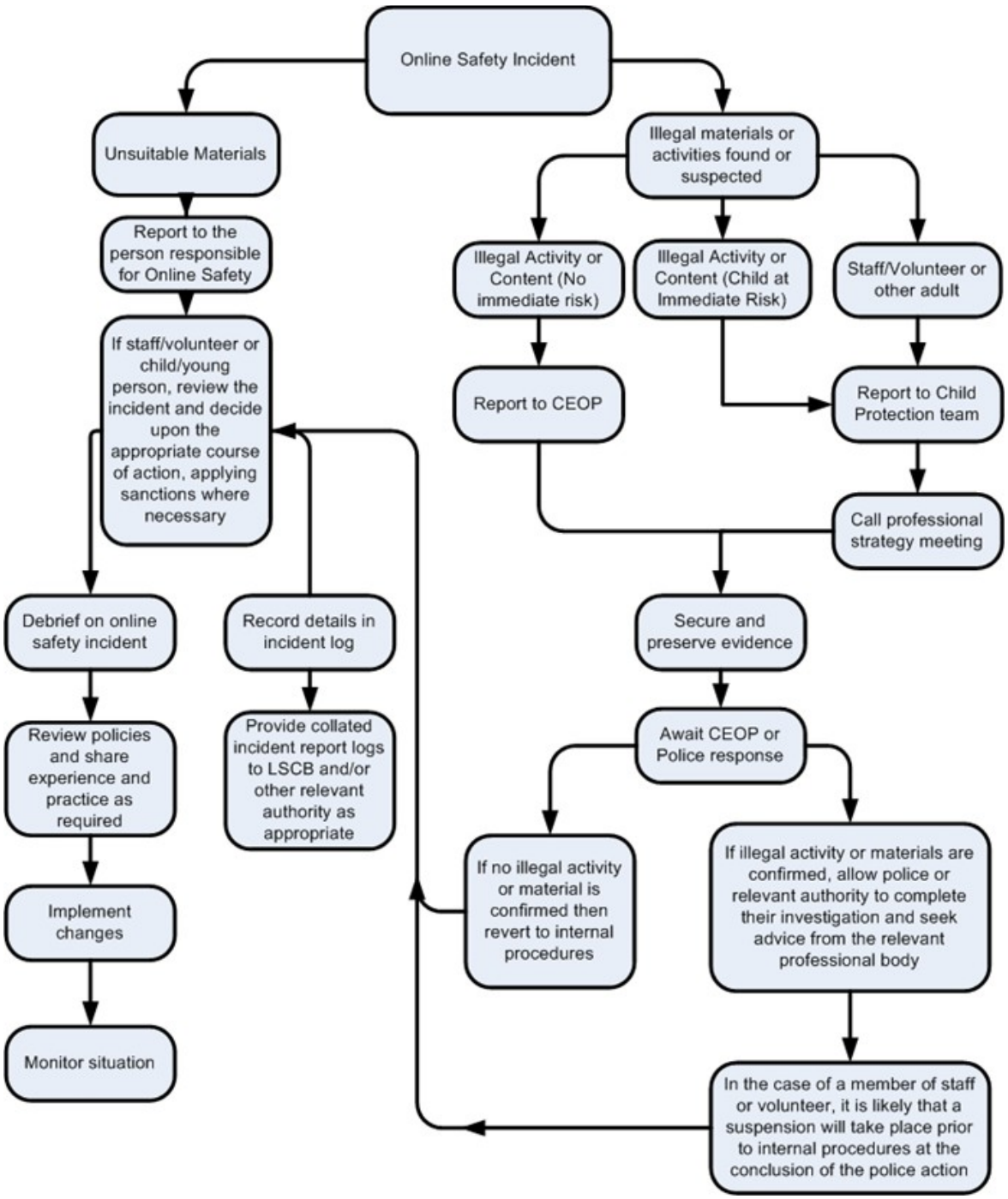
Date: January 2018
Amended: January 2021

Appendix 1: Roles and Responsibilities

Role	Responsibility
Governors	Approve and review the effectiveness of the online safety policy and acceptable use policies Receive reports regarding the monitoring of the policy and any incidents arising
Head teacher and Senior Leaders:	Duty of care to ensure the safety (and online safety) of the school community. The Headteacher and at least one other member of SLT should know the procedure to be followed in the event of a serious online safety allegation being made against a member of staff. Ensure that all staff receive suitable CPD to carry out their Online safety roles. Ensure that there is a system in place for monitoring and support of those who carry out the internal online safety role. Inform the local authority about any serious Online 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.
Online safety Leader	Lead the online safety working group and deals with day to day online safety issues Lead role in establishing / reviewing online safety policies / documents and checking links to other policies Ensure all staff are aware of the procedures to follow if there is an online safety incident Provide and/or broker relevant training and advice for all school staff Attend updates and liaise with the LA online safety staff and technical staff Receive reports of online safety incidents and keeps the incident log updated Report regularly to SLT Develop an online safety teaching programme to deliver the statutory programme of study. Monitor online safety teaching to ensure this is being delivered and is having an impact on pupils' understanding.
Child Protection Safeguarding Lead	Have received training in online safety issues and know the potential for child protection and safeguarding issues to arise from sharing personal data, access to illegal/ inappropriate materials, inappropriate online contact with strangers, potential or actual incidents of grooming and cyber-bullying.
Curriculum Leaders	Ensure online safety is appropriately reflected in teaching programmes where relevant eg anti bullying, English publishing and copyright and is reflected in relevant policies.
Teaching and Support Staff	Ensure they have an up to date awareness of school online safety issues, policies and practices. Have read, understood and signed the Staff Acceptable Use Agreement (AUP) Act in accordance with the AUP and Online safety policy Report any suspected misuse or problem to the Headteacher / online safety leader. In the event that the incident involves the Headteacher report to the Chair of Governors. Only communicate with pupils / parents / carers professionally through official school systems Ensure online safety issues are embedded in the curriculum and other activities Ensure pupils follow the online safety rules Ensure that the school programme of study for online safety is delivered through their teaching Monitor ICT activity in lessons, extra-curricular and extended school activities Deliver the scheme of work for online safety and ensure children have a good understanding of what they are being taught. Monitor use of digital technologies (mobile devices and cameras etc) in lessons and other school activities where their use if allowed and implement policies about their use. Ensure that students are guided to appropriate sites in pre-planned internet use, that they are aware of how to search more safely and that any unsuitable material that is accessed is dealt with according to school policy. Immediately report any issues in accordance with school policy.
Students / pupils	Use schools systems in accordance with the pupil acceptable use policy Practice age-appropriate safe searching in order to reduce access to unsafe material Understand how to report online safety issues and do this immediately when an issue

	arises Know and follow the policies on use of mobile devices and cameras including taking images. Understand the importance of using technologies safely outside school and know that the policy covers actions out of school that are related to their membership of the school Help their friends to keep safe by pointing out any risks and what they could do about them
Parents and carers	Read the school guidance about online safety in the newsletter and on the website and take appropriate action if required to keep their child safe. Endorse (by signature) the Pupil Acceptable Use Policy Ensure that their child / children follow appropriate acceptable use rules at home Discuss online safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet Access the school website / online platform in accordance with the relevant school Acceptable Use Policy. Keep up to date with issues through school updates and attendance at events Ensure they follow the school policy on taking digital and video images at school events Ensure their children following rules on appropriate use of children's own devices in school Report any online safety issues that could impact on safeguarding of any children or learning in school so that the school can put in place appropriate measures and use these to inform any changes to teaching
Technical Support Provider	Ensure the school's ICT infrastructure is secure and is not open to misuse or malicious attack Ensure that the school meets Online safety technical requirements of the LA Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly changed Ensure that filtering is robust is blocking but does not inhibit learning and teaching Keep up to date with online 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 head teacher / online safety leader 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 take action to prevent spyware and malware.
Community Users	Sign and follow the AUP before being provided with access to school systems.

Appendix 2: reporting procedure



Appendix 3: Actions and Sanctions: Pupils

Pupils — Actions / Sanctions

Incidents:	Refer to class teacher	Refer to Key Stage Leader	Refer to Headteacher /	Refer to Police	Refer to technical support staff for action re filtering / security	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X					X			
Unauthorised use of mobile phone / digital camera / other mobile device		X	X			X			
Unauthorised use of social media / messaging apps / personal email		X				X			
Unauthorised downloading or uploading of files		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	
Attempting to access or accessing the school network, using the account of a member of staff									
Corrupting or destroying the data of other users	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
Continued infringements of the above, following previous warnings or sanctions			X			X			X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X			X			X
Using proxy sites or other means to subvert the school's 's filtering system			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
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X			X			X

Appendix 4: Actions and Sanctions: Staff/other users

Staff/other users

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal		X	X	X		P	P
Inappropriate personal use of the internet / social media / personal email		X				P	P
Unauthorised downloading or uploading of files		X				P	P
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				P	P
Careless use of personal data eg holding or transferring data in an insecure manner		X				P	P
Deliberate actions to breach data protection or network security rules		X				P	P
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X		X		P	P
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X			P	P
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		X				P	P
Actions which could compromise the staff member's professional standing			X			P	P
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X			P	P
Using proxy sites or other means to subvert the school's 's filtering system			X			P	P
Accidentally accessing offensive or pornographic material and failing to report the incident			X	P		P	
Deliberately accessing or trying to access offensive or pornographic material			X	X		X	X
Breaching copyright or licensing regulations		X				P	P
Continued infringements of the above, following previous warnings or sanctions			X			X	X

P = possible

Appendix 5: E-Safety Audit

This quick self-audit is used to help the senior management team (SMT) assess whether the e-safety basics are in place and enables us to monitor safety.

Has the school an e-Safety Policy that complies with CFE guidance?	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents at:	
The Designated ~~Child Protection Coordinator~~Safeguarding Lead is:	
The e-Safety Coordinator is:	
Have roles and responsibilities in relation to e-safety been clearly identified?	Y/N
Has e-safety training been provided for both students, staff and parents? How frequently? Has it highlighted any issues?	Y/N
Do all staff sign an ICT Code of Conduct on appointment? Do you have one?	Y/N
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Y/N
Have school e-Safety Rules been set for students which have been discussed with them?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DCfS requirements for safe and secure access (e.g. SWGfL).	Y/N
Has an ICT security audit has been initiated by SL~~M~~T, possibly using external expertise?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Has monitoring of internet use taken place with any issues being logged?	Y/N
Has an e-safety log been completed and reviewed to identify and issues which need to be addressed?	Y/N
The self-review framework has been completed this year in order to identify and respond to any issues	Y/N
Relevant pupil surveys have been completed and issues have been identified and addressed through teaching	Y/N

Appendix 7: Acceptable Use Policy (Pupils)

I know that I should never allow anyone to use my password and that I should keep it any other personal information private.

Finding information on the internet safely

I know:

- That being responsible means I should not try to visit unsafe sites or register for things I am not old enough for
- That any protection system does not stop all unsafe content
- What to do if I open something that I don't like
- How to search safely to find the information I want
- That I should be supervised to ensure I am keeping safe
- That any information I put up on the web can be read be anyone
- That I should ask permission to use the work of others and credit them if I do
- That I should not copy others work and claim it as my own

Using technology to contact people

I know:

- To choose my user name carefully to protect my identity
- To keep my personal information private
- Not to take/use pictures of people without their permission
- To use safety features of web sites
- To limit access to my personal information
- That e-mails / messages can be intercepted and forwarded on to anyone
- That I should be careful who I add as friends
- That I need to be polite online and friendly online and think about the language I use (it could be forwarded to my parents or head teacher!)
- To use the subject field in e-mails
- Not to open messages if the subject field contains anything offensive or if I do not recognise who it is from (delete it without opening it)
- What to do if I receive an offensive message / e-mail including how to keep evidence
- That people online may not be who they seem

Using technology to for buying and selling

I know:

- How to tell the difference between web sites for information and web sites selling things
- How to recognise commercial uses of the internet e.g. I Tunes, mobile phone downloads, shopping
- Not to leave computers logged on with my user name or logged on to sites with personal details entered
- That if an offer looks too good to be true it probably is
- That I should not respond to unsolicited online offers
- That I should not use someone else's identity to buy things online

Signed (KS2 only):_____ **Date:** _____

Appendix 8: Acceptable Use Policy (Staff, Volunteers, other users)

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.

Use of school system

- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal use within the policies and rules set down by the school.
- I will be professional in my communications and actions when using school ICT systems:
- I understand that the school may monitor my use of the school's ICT systems, school email and other digital communications operated by the school.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, class dojo) out of school.
- I understand that I must not communicate information which is confidential to the school or which I do not have the authority to share.
- I understand that I must not use the school ICT system to access inappropriate content, or for personal financial gain, gambling, political activity, advertising or illegal purposes.
- I will report any incidences of concern regarding children's safety to the Designated Safeguarding Lead/Headteacher.
- I will report any incidences of inappropriate use of ICT and inappropriate electronic communications, whether by pupils or colleagues, to the Headteacher, or if appropriate, the Chair of Governors.

Security

- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
- I will not install any software or hardware without permission.
- I will follow the school's policy in respect of downloading and uploading of information and material.
- I will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely. I will not routinely keep personal data on removable storage devices. Where personal data is required, it will be password protected/encrypted and removed after use.
- I will respect copyright, intellectual property and data protection rights.

Social networking/use of social media

- 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 and when personal equipment has been used for such purposes, images will be transferred to the school network and then deleted from the device as soon as is reasonably possible.
- I will ensure that any electronic communication undertaken on behalf of the school, including email and instant messaging are compatible with my professional role and that messages do not present personal views or opinions and cannot be misunderstood or misinterpreted.
- I understand the school's stance on use of social networking (see separate policy) and, given my professional role, will exercise care in any personal use of social networking sites.
- I will not communicate with pupils directly or indirectly using email or social networking sites.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

I understand that inappropriate use of personal and other non-school based ICT facilities can have implications for my employment at the school (where relevant). I understand that the use of any personal device (eg phone) must not conflict with my role in school.

Name……

Signed …… Date ……..

Appendix 9: Guide for parents

Monitoring Home Use of the Internet

Parents / carers should:
- Ensure that young people access the internet in a communal room
- Ask their children about what sites they are looking at
- Ensure that family computers are password protected and have robust anti-virus software which is regularly updated
- Ensure content is appropriately filtered for younger users

Content – finding and publishing information on the internet

Parents / carers should:
- Ensure that their children know that they will only get to use the internet if they use it responsibly and that being responsible means they should not try to visit unsafe sites or register for things they are not old enough for.
- Ensure that their children know that any protection system does not stop all unsafe content and that children need to tell them if they access something inappropriate.
- Encourage children to search safely to find the information they want and search safely themselves using very specific search terms to reduce the likelihood of accessing unsafe material.
- Supervise younger children when they are using the internet
- Talk to children about the fact that any information published on the web can be read be anyone
- Check information that younger users are publishing on the web before it is posted to ensure that they are not putting themselves in danger

Contact - Using technology to contact people

Parents / carers should:
- Discuss user names with children and talk about how to choose them carefully to avoid putting themselves at risk and protect their identity
- Identify the information that young people should keep private in order to prevent them being contacted or traced including
- Talk to children about the need to use safety features of web sites
- Talk to their children about limiting access to their personal information
- That e-mails / messages can be intercepted and forwarded on to anyone
- should talk to their children about being careful who they add as friends
- Talk about the need to be polite online and friendly online and think about the language they use (it could be forwarded to my parents or head teacher!)
- Discuss how to use the subject field in e-mails
- Not to open messages if the subject field contains anything offensive or if I do not recognise who it is from (delete it without opening it)
- Discuss what to do if I receive an offensive message / e-mail including how to keep evidence
- Explain that people online may not be who they seem