Elm Park Primary School

Inspiring Learners, Enriching Lives, Achieving Together

Online Safety and Acceptable Use Policy

Written/revised by	Josh Bartlett & Deb Williams / Jo Briscombe & Andrew Evans Sept 2018
Start Date	Jan 2019
Reviewed Date	February 2022
Headteacher's Signature	
Chair of Governors' Signature	
Date ratified by FGB	14/1/19

Online Safety and Acceptable Use Policy

This online safety policy has been developed, and will be reviewed and monitored from September 2017, by our school online safety working group which will comprise of:
- Current Computing Subject Leader / The Online Safety Lead (Mrs M Keeping / Mr A Evans)
- Current DSL / DDSL (Mr A Evans/ Mrs C Bond)
- Current Headteacher (Mr A Evans).
- A representative of SLT / teaching or support staff.
- A governor representative.

Consultation with the whole school community will take place through a staff meeting, School Council meeting, governors meeting, direct communication with parents and the school website / newsletter.

Schedule for Monitoring and Review

Policy ratified by the *Governing Body on:*	
The implementation of this policy will be monitored by:	Online safety working group
Monitoring will take place:	Annually
The *Governing Body* will receive a report on the implementation including reported incidents:	Annually at FGB in Term 6
This policy will be reviewed:	Annually during Term 1
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 various sources, including:
- Logs of reported incidents and responses.
- Monitoring logs of internet activity and any network monitoring data.
- Surveys / questionnaires of students 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 governors and senior leaders to ensure that it complies with this policy and the Acceptable Use guidelines.
- Any other web site, such as the PTFA, that is linked to the school name is also 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 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 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 present. 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 Learning & Standards 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. 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.

Training and Awareness Raising

There is a planned programme of online safety training for **all** staff and governors to ensure that they understand their responsibilities, as outlined in this, and the Acceptable Use policy. The following actions are undertaken to raise awareness:

- An audit of the online safety training needs of all staff is carried out regularly.
- The DSL and Online Safety Leader receive regular updates through attendance at relevant training such as SWGfL and LA training sessions and by receiving regular online safety updates from the South Gloucestershire Traded Services.
- All staff, including support staff, receive an annual online safety update alongside their safeguarding & KSIE training
- Any reported incidents and how they are addressed are discussed at staff meetings and used as an opportunity to test our processes and update staff on how to deal with issues.
- The Online Safety Leader provides advice/guidance and training as required to individuals and seeks LA advice on issues where appropriate.
- A training log is used to record when updates and training are delivered.

Induction Processes

- All new staff receive online safety training as part of their induction programme.
- Parents of new reception children receive information about online safety and processes as part of their induction meeting when their child starts school. These are entitled, "Parent/Carer Acceptable Use Policy" and "Home Use of the Internet". From Term 6 2019 onwards an annual update will be sent to all current parents YR-Y6.
- Parents of children who join school mid-year will be similarly made aware of the processes and will be provided with the Acceptable Use Policy / Parent guidelines.

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 other lessons. 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 PSHE, assemblies and events. Older pupils are taught to acknowledge the source

of information and respect copyright. Pupils are helped to understand the 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 a clearly logged with reasons given for this access.
Children new to the school are provided with an overview of expectations when they start.

The following aspects also contribute to our curriculum provision:
- Coverage of learning experiences is recorded and staff check understanding when teaching about online safety.
- Annual online safety events such as Safer Internet Day (in February each year) are also used to raise awareness.

Rules for Keeping Safe
These are reinforced through the following:
- In 2018-2019 academic year, the school will revise the acceptable use agreement for pupils as part of wider review around our home-school agreement. All pupils will be supported to understand and sign this before July 2019. The parent AUP guidelines will also be updated and both documents will be communicated to parents to reinforce the messages at home. In future years, annual updates will be sent to parents and children will re-sign at the start of Term 1.
- 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 classrooms and staff regularly refer to these, for example, during activities where children are searching the internet for information. Rules are also displayed in other areas where ICT is used.
- 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. There are sanctions and rewards in place for this.

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:
- 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 events.
- Events such as Safer Internet Day.
- Providing information and weblinks about where to access support on the website.

Parents of children new to the school are signposted to the school website to relevant policies including online safety, when their child starts school.

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, 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.
- All new staff receive online safety training as part of their induction programme.
- The Online Safety Leader receive 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 Online Safety Leader provides 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.
- 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 any number of the following:
- Local authority annual safeguarding audit.
- Surveys with pupils and staff.
- (In 2018-2019 the school will research the use of the 360 degree safe online self-evaluation tool which can also be used to benchmark our provision against other schools).

Technical Issues
The local authority provides technical and curriculum guidance for online safety issues for **all** 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. 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**.
Individual log-ins are similarly used to access our governor online portal area and computing scheme of work.
Access to systems is through groups so that only the relevant group of users can access a resource.

Internet Provider and Filtering
The South Gloucestershire school internet service is provided by Integra and this includes a filtering service to limit access to unacceptable material for all users. Internet access is filtered for all users by South Gloucestershire School IT. 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.
- Any filtering requests for change and issues are also reported immediately to the South Gloucestershire technical team on 3838.
- Requests from staff for sites to be removed from the filtered list must be approved by the Headteacher and this is logged and documented by a process that is agreed by the Headteacher.

The school is currently implementing a technical monitoring solution through the local authority in order to fulfil the requirements within Keeping Children Safe in Education. The iBoss solution being implemented provides the following:
- active monitoring and automatic alerts for the school to act upon, together with pro-active monitoring by Integra Schools IT to support the school by drawing attention to concerning behaviours, communications or access.
- enhanced filtering integrated with the police assessed list of unlawful terrorist content, produced on behalf of the Home Office.
- delegated access to the filtering system allows us to permit or deny access to specific content to support the requirement that "over blocking" does not lead to unnecessary restrictions on what can be taught relating to online teaching and safeguarding - the most severe content will always be filtered.
- network level filtering which does not rely on any software on the users' devices which could be disabled
- ability to produce reports on the websites visited by all young people and adults using our systems.
- the ability for alerts to be set so that a number of people are informed when they are triggered meaning that monitoring does not need to fall into the remit of only one person which could result in issues being missed or covered up.

- external alerts to people outside the school (such as safeguarding, online safety officers or IT technicians) so that monitoring is not reliant wholly on school staff and appropriate actions can be taken immediately to safeguard children and staff.
- automated reporting to ensure that processes are followed without fail.
- ability to log in from anywhere to see reports via web interface.

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 is 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 ICT systems.
- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All users have clearly defined access rights to school ICT 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 onto the school system is provided for "guests" (e.g. student teachers, supply teachers) at the Headteacher's discretion.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT 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.
- Staff are not allowed to install programmes on school workstations / portable devices. The Computing Leader manages the installation and removal of educational apps.
- Staff are advised regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations/portable devices in our staff Acceptable Use Agreement and through GDPR training support. Aal staff have remote access to the school system through and encrypted password and 2 step authentication using Microsoft authenticator.

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 are much easier and if not managed, this could increase the potential 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 for 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 on school equipment (but not on their own technology) 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. 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 AND reminders are given to parents at the start of whole-school events eg Nativity Plays and Concerts.

- Parents are asked for their permission to include photographs of their children on Tapestry for children in EYFS.

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.

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 to telephone, or when for cover reasons, staff in classes need to be able to contact the office (when it has been agreed by a member of the senior leadership team). At lunchtimes the Lunch Break Supervisors have access to a mobile phone to contact the school office in case of emergency only.

Staff should not use their own mobile phone to take images of children, for example, on a school trip as the school has devices available for this.

Communication Technologies and Social Media

A wide range of communication 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.
- All governor email communication takes place via sgmail and/or the Teams portal. Governor data and information traffic has been much reduced through the use of the secure Governor portal; this is in line with the school's GDPR improvement work. Personal or sensitive information is not e-mailed.
- Personal email addresses, text messaging, public chat and social networking programmes are not be used for communications with parents/carers and children.
- 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 the responsibility of the Computing Leader.
- 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 personal use of social media where it does not relate to the school is outside the scope of the policy, but it 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.
- The Online Safety Leader pro-actively monitors the Internet for postings about the school.

Copyright

The Online Safety Leader 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 relates 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.

Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998 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

See Data Protection policy.

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.

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 and staff access it online through Ericom.
- Personal data including assessment data is transferred using secure file transfer.
- 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 Data Protection Act (DPA).
- There is 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 procedure 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.
- 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 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 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 DSL 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.
- Where an allegation is made about staff, the LADO should be informed (8508).

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:
  o incidents of 'grooming' behaviour.
  o the sending of obscene materials to a child.
  o adult material which potentially breaches the Obscene Publications Act.
  o criminally racist material.
  o promotion of terrorism or extremism.
  o 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 Leader 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
> 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. Schools are advised to adapt these to suit their own circumstances.

Appendix 1: Roles and Responsibilities

Role	Responsibility
Governors	Approve and review the effectiveness of the Online Safety policy and Acceptable Use policies Online safety governor works with the Online Safety Leader to carry out regular monitoring of online safety incident logs, filtering, changes to filtering and then reports to governors.
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 deal 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. Receives reports of online safety incidents and keeps the incident log updated. Meet with online safety governor to regularly to discuss issues, review the incident log and filtering / changes to filtering log. 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 governor responsible for safeguarding. 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 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 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.