WEST RISE

WEST RISE JUNIOR SCHOOL

POLICY: E-Safety

Date of Policy: September 2017

Ratified by Governors: 12th September 2017

Signed by Chair of Governors ____________________

Review Date: Septemberber 2018

At West Rise Junior School we inspire and empower independent and creative learners who will continue to enrich their lives and those of others within a culture of high achievement and mutual respect.

At West Rise Junior School we aim to identify and support all pupils following guidance laid out in the East Sussex Dyslexia Policy.

West Rise Junior School is a Rights Respecting School and puts the articles of the Unicef Children's Rights Charter at the heart of all school policy. This policy reflects that as a school we recognise that all children have the right to be safe, be educated and learn, be treated fairly, be listened to, a healthy lifestyle, extra support if they need it and a right to join in cultural and artistic activities.

DEVELOPMENT/MONITORING REVIEW OF POLICY

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

- School E-Safety Coordinator
- Headteacher
- Teachers
- Support Staff
- ICT Technical staff
- Governors
- Parents and Carers
- Senior Management Team

Consultation with the whole school community has taken place through the following:

- Staff meetings

- Pupil Council
- E-Safety Training Day
- Governors meeting
- Parents drop-in session

SCHEDULE FOR DEVELOPMENT / MONITORING / REVIEW

This E-Safety policy was approved by the Governing Body on:	Insert date
The implementation of this E-Safety policy will be monitored by the:	E-Safety Coordinator: Helen Pentecost Senior Management Team:
Monitoring will be an ongoing matter	
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to E-Safety or incidents that have taken place. The next anticipated review date will be:	November 2016
Should serious E-Safety incidents take place, the following external persons / agencies should be informed:	LA ICT Manager LA Safeguarding Officer Police Commissioner's Office

The school will monitor the impact of the policy using:

- Logs of reported incidents

STATEMENT OF DEFINITION

All people working in the school should be aware of E-Safety at all times, know the required procedures and to act on them. E-Safety is not limited to the school premises, school equipment or the school day, neither is it limited to equipment owned by the school, which is why it is important that we work in a partnership with parents and carers. E-Safety is therefore a partnership concern, as an incident occurring outside school and brought to the school's attention will be treated as if it happened on school premises in the teaching day.

STATEMENT OF CARE

Members of the School Management Team have responsibility for all E-Safety matters and all staff within the school have a responsibility to support E-Safety practice in the school. Children at all levels need to understand their responsibilities and liabilities in the event of deliberate attempts to breach E-Safety protocol, and in these instances this must be referred to members of the School Management Team.

SCOPE OF POLICY

- E-Safety concerns the day to day running of the physical network and information passing through it whether connected via the internet, virtual private networks, intranets or local area networks.
- There will be an emphasis on the children being taught safe practice in lessons, and how this should be applied with use of the internet etc outside of school in order to keep themselves safe.
- The E-Safety policy will be reviewed and monitored annually by the Computing co-ordinator and members of the School Management Team.
- E-Safety covers technology not owned by the school, and the school will respond to E-Safety threats involving members of the community whether they occurred during the school day, on the school site or if perpetrated using equipment not owned or operated by the school.
- When children enter the school, parents and carers must sign the agreement to home school agreement, school policies/contracts if their children are to use the internet at school.

ROLES AND RESPONSIBILITIES

The following section outlines the roles and responsibilities for E-Safety 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. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- Regular meetings with the E-Safety Co-ordinator / Officer
- Regular monitoring of E-Safety incident logs
- Reporting to relevant Governors committee / meeting

Headteacher and Senior Management Team:

- The Headteacher is responsible 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 Coordinator.
- The Headteacher/Senior Management Team are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues.
- The Headteacher / Senior Management Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Management Team will receive regular monitoring reports from the E-Safety Co-ordinator.
- The Headteacher and another member of the Senior Management Team 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.

E-SAFETY COORDINATOR:

- Takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies.
- 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 ICT co-ordinator and outside technical support.
- Receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments.
- Meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs.
- Attends relevant meeting / committee of Governors.
- Reports regularly to Senior Management Team.

NETWORK MANAGER:

It is the responsibility of the school to ensure that the managed service provider carries out all the E-Safety measures that would otherwise be the responsibility of the school's technical staff. It is also important that the managed service provider is fully aware of this policy.

The Network Manager is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets the E-Safety technical requirements outlined in this policy.
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed. Individual passwords for all children has proved impossible to maintain and therefore a new system has been put in place: Each year group has its own log in; all laptops are numbered; each class has a list of which laptop each child may use and they are only to use that laptop; when children work in pairs/groups they must be using one of the groups numbered laptop only. Should an E-Safeguarding issue arise this will narrow down the possible parties to only 2 or 3 in a year group making dealing with any issues much more manageable.

- that he / she keeps up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant.
- that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator.
  - Staff are reminded to change their passwords every 90 days.

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 E-Safety policy and practices.
- They have read, understood and signed this policy.
- They report any suspected misuse or problem to the E-Safety Co-ordinator for investigation.
- Digital communications with students / pupils (email / school blogs and website / voice) should be on a professional level.
- E-Safety issues are embedded in all aspects of the curriculum.
- Students / pupils understand and follow the school E-Safety and acceptable use policy.
- They monitor ICT activity in lessons, extra curricular and extended school activities.
- They are aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- 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. Pupils should use the Safe Search website (primaryschoolict.com) which is accessible from the school website.

CHILD PROTECTION OFFICER:

The child protection officer will take on the role of E-Safety Officer too. They should be trained in E-Safety issues and be 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.
- cyber-bullying.

STUDENTS/PUPILS:

- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through one parents' drop in session, newsletters, letters, website and information about national / local E-Safety campaigns. Parents and carers will be responsible for:

- **endorsing (by signature) the Student / Pupil Acceptable Use Policy.**
- accessing the school website and school blogs in accordance with the relevant E-Safety and School Acceptable Use Policy.

EDUCATION – STUDENTS/ PUPILS

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of students / pupils in E-Safety is therefore an essential part of the school's E-Safety provision. Children and young people need the help and support of the school to recognise and avoid E-Safety risks and build their resilience.
E-Safety education will be provided in the following ways:

- A planned E-Safety programme should be provided as part of ICT / PHSE lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key E-Safety messages should be reinforced as part of a planned programme of assemblies to co-inside with national / local E-Safety campaigns.
- Pupils should be helped to understand the need for the pupil Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Rules for use of ICT systems / internet will be discussed and agreed with the children in each class and these will be displayed in each classroom alongside the Class Charter.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

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 experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).
The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, school blogs.
- Parents drop-in session

EDUCATION AND TRAINING - STAFF

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:

- An audit of the E-Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify E-Safety as a training need within the performance management process.
- 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 Policies.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required.

TRAINING - GOVERNORS

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

- Participation in school training / information sessions for staff or parents.

TECHNICAL – NETWORK/EQUIPMENT, FILTERING AND MONITORING

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their E-Safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the E-Safety technical requirements outlined in this policy.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers must be securely located and physical access restricted.

- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, every six months, by the E-Safety Officer.
- Pupils will gain access to the school network by logging onto their year group. They are to only use the laptop allocated to them (each laptop is numbered and all children have been allocated a number). In the event of paired or group work a laptop allocated to one of that group must be used.

In Year 4 each pupil is provided with a username, password and email address. Use by pupils in this way should always be supervised and members of staff should never use a class log on for their own network access.

The passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher and kept in a secure place.

- Users will be made 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.
- In the event of the Network Manager needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.

- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and the ICT Coordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Senior Management Team.
- An appropriate system is in place for users to report any actual / potential E-Safety incident to the Network Manager or ICT Coordinator. These reports should be written and given to the Network Manager and ICT Coordinator.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system.

An agreed policy is in place regarding the downloading of executable files by users.

- An agreed policy is in place 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.
- Staff are not allowed to install programmes on school workstations / portable devices unless approved by the network manager.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

CURRICULUM

E-Safety should be a focus in all areas of the curriculum and staff should reinforce E-Safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use. The search engine Safe Search (primaryschoolict.com) should be used when using the internet. This is accessible through the school website.
- Where students / pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit. Staff should remind pupils to report anything unsuitable immediately and then complete the incident form found on both the LearnPad and laptop trolleys and give it to Mrs Poore to action.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT coordinator can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. The Network Manager will need to be told of these changes.
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

USE OF DIGITAL AND VIDEO IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students / pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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 eg school blogs or the school website.**
- Staff are allowed to take digital / video images to support educational aims. 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 staff permission.
- Photographs published on the website, or elsewhere that include students / 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 is requested before photographs of pupils are published on the school website or school blogs. Parents/ carers are also asked to sign the Parents / Carers Agreement in the appendix before pupils are put on the school website or blog however permission is implied if the forms are not returned.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Parents are permitted to take photographs at major school events but must comply with the I.C.O guidance on sharing these photos. For the full details on this guidance please click on the link http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/taking_photographs_in_schools.pdf .

DATA PROTECTION

Staff must ensure that they:

- At all times take care to ensure the safe keeping of school data, minimising the risk of its loss or misuse.
- Use school 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 school data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected).

- The data must be securely deleted from the device once it has been transferred or its use is complete.

COMMUNICATIONS

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X					X		
Taking photos on cameras	X							X
Use of personal email addresses in school, or on school network				x				X
Use of school email for personal emails		X						X
Use of social networking sites		X						X
Use of personal blogs				x				x
Use of school related blogs	x				X			

When using communication technologies the school considers the following as good practice:

- **The official school email service may be regarded as safe and secure.**
- **Users need to be aware that email communications may be monitored.**
- **Users must immediately report, to the Headteacher the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.**
- **Any digital communication between staff and students / pupils or parents / carers (email, chat, class blogs etc) must be professional in tone and content.** Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils from Year 4 onwards will be provided with individual school email addresses for educational use.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

UNSUITABLE/INAPPROPRIATE ACTIVITIES

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities eg Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. Reported cases of inappropriate activities may be referred to the police for further investigation.

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 certain internet usage as follows:

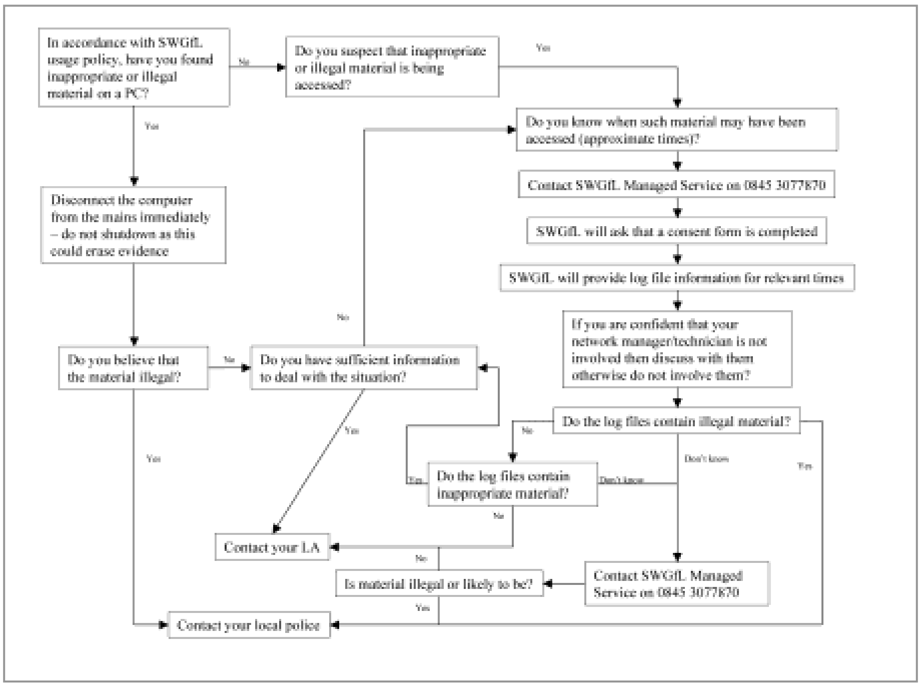
User Actions		Acceptable	Unacceptab	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**child sexual abuse images**			X
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation			X
	adult material that potentially breaches the Obscene Publications Act in the UK			X
	criminally racist material in UK			X
	Pornography		X	
	promotion of any kind of discrimination		X	
	promotion of racial or religious hatred			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	
Creating or propagating computer viruses or other harmful files			X	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet			X	
On-line gaming (educational)		X		
On-line gambling			X	
On-line shopping / commerce			X	
Use of video broadcasting eg Youtube		X		

RESPONDING TO INCIDENTS OF MISUSE

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

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


In accordance with SWGfL usage policy, have you found inappropriate or illegal material on a PC?
No
Do you suspect that inappropriate or illegal material is being accessed?
Yes
Yes
Do you know when such material may have been accessed (approximate times)?
Contact SWGfL Managed Service on 0845 3077870
Disconnect the computer from the mains immediately – do not shutdown as this could erase evidence
SWGfL will ask that a consent form is completed
SWGfL will provide log file information for relevant times
No
If you are confident that your network manager/technician is not involved then discuss with them otherwise do not involve them?
Do you believe that the material illegal?
No
Do you have sufficient information to deal with the situation?
Do the log files contain illegal material?
No
Yes
Yes
Don't know
Yes
Yes
Do the log files contain inappropriate material?
Don't know
No
Contact your LA
No
Is material illegal or likely to be?
Contact SWGfL Managed Service on 0845 3077870
Yes
Contact your local police

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

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

Incidents:	Refer to class teacher	Refer to Headteacher	Headteacher to Refer to Police	Refer to Network Manager	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		X	
Unauthorised use of non-educational sites during lessons	x	X					X	
Unauthorised use of mobile phone / digital camera / other handheld device	X	X					X	
Unauthorised use of social networking / instant messaging / personal email	X	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 student's / 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	
Corrupting or destroying the data of other users	x	x		x			X	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	x	x		x	x		x	X
Continued infringements of the above, following previous warnings or sanctions	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
Using proxy sites or other means to subvert the school's filtering system	x	x		x			x	X
Accidentally accessing offensive or pornographic material and failing to report the incident	x	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	x		x	X

Staff

Incidents:	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Network Manager	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		x	x	X
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	x				X		
Unauthorised downloading or uploading of files	x				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			x	x	x	X
Careless use of personal data eg holding or transferring data in an insecure manner	x			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 instant 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
Actions which could compromise the staff member's professional standing	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 filtering system	x			x			X
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x		x	X		
Deliberately accessing or trying to access offensive or pornographic material	x	x		x	x	x	X

Breaching copyright or licensing regulations	x			X			
Continued infringements of the above, following previous warnings or sanctions	x	x				x	X

PROCEDURES TO BE FOLLOWED IN THE EVENT OF A BREACH OF E-SAFETY

All instances of E-Safety, whether by direct observation or disclosure will be taken seriously. In these instances, it must be reported immediately to members of the School Management Team who will deal with the situation as appropriate. All instances where there is a breach of E-Safety must be logged and kept on record. The Child Protection Policy should be referred to when there are child protection concerns and a serious breach of the E-Safety policy, and appropriate disciplinary procedures followed as set out in these guidelines. In instances where there is a breach of E-Safety, the E-Safety incident reporting form (See appendix) must be completed and passed on the Head Teacher.

The Physical Environment

All wireless networks within the school are encrypted to WPA2 standard. All subcontractors installing Wireless Access Points demonstrate required encryption in place.

Password Policy

All new staff must change their password for their username on the school system immediately to ensure password strength Users will not log on using any other username/password other than their own. Staff will be reminded to change their passwords every 90 days.

Monitoring and Reporting Procedures

E-Safety will be monitored regularly by the ICT co-ordinator and members of the School Management Team. The E-Safety policy will be reviewed annually by the ICT co-ordinator and the School Management Team. All breaches of E-Safety will be logged and recorded. These will be shared with legitimate agencies as necessary to ensure E-Safety is upheld within the school. In instances where there is a breach of E-Safety, the E-Safety incident reporting form must be completed and passed on the Head Teacher.

Advice to Parents

- As E-Safety needs to be addressed in partnership with parents and carers, then it is important that the school are able to provide advice and support them with E-Safety. The school is willing to advise parents and carers on home wireless links, location of computers, internet service provider child controls and anti-virus/ spyware and malware. The school is able to provide advice, but does not accept responsibility for computers and software that is not used on the school property. There will be a section on the school website with information aimed at parents.

PUPIL ACCEPTABLE USE POLICY AGREEMENT

This Acceptable Use Policy is intended to ensure:

- that young people 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.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my mobile phones / USB devices in school if I have permission. I understand that, if I do use my own devices in school, once I obtain permission I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will only use chat and social networking sites with permission and at the times that are allowed.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Policy (AUP), to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) eg mobile phones, memory card, cameras.
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, school blogs and website.

Name of Student / Pupil

Class

Signed

Date

STAFF (AND VOLUNTEER) ACCEPTABLE USE POLICY AGREEMENT

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed E-Safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, school website, school blogs) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images (within this policy.) I will not use my personal equipment to record these images. Where these images are published (eg on the school website / school blog) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's social media policies.
- 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.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.

- I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not (unless I have permission) make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

PARENT/CARER ACCEPTABLE USE POLICY AGREEMENT

This Acceptable Use Policy is intended to ensure:

- that young people 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 parents and carers are aware of the importance of E-Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that students / pupils will have good access to ICT to enhance their learning and will, in return, expect the students / pupils to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above students / pupils, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter will has signed an Acceptable Use Agreement and has received, or will receive, E-Safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's E-Safety.

Signed Date

Please note: If the school **does not** receive this form back permission to publish photos will be implied.

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people can not be identified by the use of their names.

Parents are permitted to take photographs at major school events but must comply with the I.C.O guidance on sharing these photos. For the full details on this guidance please click on the link http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/taking_photographs_in_schools.pdf .

Parents are requested to sign the permission form below to allow the school to take and use images of their children.

Permission Form

Parent / Carers Name	
Student / Pupil Name	

As the parent / carer of the above student / pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed		Date	

E-Safety – A School Charter for Action

Name of School

Name of Local Authority

We are working with staff, pupils and parents / carers to create a school community which values the use of new technologies in enhancing learning, encourages responsible use of ICT, and follows agreed policies to minimise potential E-Safety risks.

Our school community
Discusses, monitors and reviews our E-Safety **policy** on a regular basis. Good practice suggests the policy should be reviewed annually or at most every two years.

Supports **staff** in the use of ICT as an essential tool for enhancing learning and in the embedding of E-Safety across the whole school curriculum.

Ensures that **pupils** are aware, through E-Safety education, of the potential E-Safety risks associated with the use of ICT and mobile technologies, that all E-Safety concerns will be dealt with sensitively and effectively; that pupils feel able and safe to report incidents; and that pupils abide by the school's E-Safety policy.

Provides opportunities for **parents/carers** to receive E-Safety education and information, to enable them to support their children in developing good E-Safety behaviour. The school will report back to parents / carers regarding E-Safety concerns. Parents/carers in turn work with the school to uphold the E-Safety policy.

Chair of Governors

Headteacher

E-SAFETY INCIDENT REPORTING FORM

Date of Incident	
Member of staff reporting the incident	
Location of incident	
Details	
URL/ web address of incident	
Incident referred to	
Action taken as a result	

- Never retaliate to online abuse/personally engage with online abuse.
- Keep any records of the abuse – web site, screen shots, printouts of web pages, date, time and URL (web) address.
- Inform the appropriate person (for example, Head of School) at the earliest opportunity.

Where the perpetrator is known and has a relationship with the school

- In the majority of cases can be dealt with most effectively by mediation between the perpetrator and the school.
- In particular, in cases where the perpetrator has been identified as the parent of a current pupil at the school it may be in the best interests of the school to maintain an appropriate relationship with that parent.
- In such cases, the school should attempt to resolve matters informally where possible; write to the parent concerned highlighting the offensive material and the reasons why that material is offensive; invite the parent to discuss their comments in a meeting with the school where possible, or otherwise to provide their views to the school via written correspondence.
- The quickest way to get material taken down is likely to be to ensure that the person who posted it understands why the material is unacceptable and to request that they remove it.
- If the person responsible will not take the material down, the school leadership team member will need to contact the web site host (for example, the social networking site) to make a report to get the content taken down. The material posted may breach the service provider’s terms and conditions of use and can then be removed.

Where the perpetrator is not known / does not have a relationship with the school

- The school leadership team member will need to contact the web site host (for example, the social networking site) to make a report to get the content taken down. The material posted may breach the service provider’s terms and conditions of use and can then be removed.
- If it is suspected that a potential criminal offence has been committed the police should be contacted. The police may then issue a RIPA (Regulation of Investigatory Powers Act 2000) request to a service provider, enabling them to disclose the data about a message or the person sending a message.

In cases where the victim's personal identity has been compromised

- For example, where a site or online identity belonging to the victim is being used, the victim will need to establish their identity and lodge a complaint directly with the service provider
- Some services will not accept complaints lodged by a third party; In cases of mobile phone abuse, for example, where the person being abused is receiving malicious calls or messages, the account holder will need to contact their provider directly.
- *Before a school or individual contacts a service provider, it's important to be clear about where the content is – for example, by taking a screen capture of the material that includes the URL or web address.*
- *If you are requesting that they take down material that is not illegal, be clear how it contravenes the site's terms and conditions.*

Where a potential criminal offence has been committed

- The police should be contacted whenever the school suspect that a criminal offence has been committed (for example: death threats, threats of assault, discriminatory/racially motivated abuse). The school should ensure that any internal investigation does not interfere with police enquiries.
- School staff are of course able to report incidents directly to the police in their capacity as private individuals.
- Department for Education Guidance[1] states:
  '*If school staff feel that an offence may have been committed they should seek assistance from the police. For example, under the Malicious Communications Act 1988, it is an offence for a person to send an electronic communication to another person with the intent to cause distress or anxiety or to send an electronic communication which conveys a message which is indecent or grossly offensive, a threat, or information which is false and known or believed to be false by the sender.*'

[1] Page 5, Department for Education Guidance: 'Preventing and Tackling Bullying' (July 2013)

Appendices

1. Guidance:

Department for Educational Guidance: 'Preventing and Tackling Bullying' (July 2013)
https://www.gov.uk/government/publications/preventing-and-tackling-bullying

Childnet International Guidance: 'Cyber bullying: Supporting School Staff'(2009)
http://www.childnet.com/resources/supporting-school-staff

Childnet International Guidance: 'CYBERBULLYING - Safe to Learn: Embedding Anti-Bullying Work in Schools' (http://www.childnet.com/resources/cyberbullying-safe-to-learn-embedding-anti-bullying-work-in-schools)

ESCC Draft Policy: 'Social Media Policy' (2012)

Draft Correspondence for Schools – Response to online abuse (2012)

2. Current Legislation:

Malicious Communications Act 1988 (section.1)

Communications Act 2003 (s.127)

Public Order Act 1986 (s.4A)

Protection from Harassment Act 1997 (s.1)

Defamation Acts 1952 (s.2), 1996 (s.1) and 2013 (s.1)

Libel Act 1843 (s.4)

Equality Act 2010