Bowhill Primary School
E-Safety Policy
Background and Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.
Our school e-safety policy helps to ensure safe and appropriate use of ICT by children at all times.

Development and Monitoring

This e-safety policy is monitored by the School e-safety Team made up of:
• Head teacher – Ms Caren Brooks
• Safeguarding - Mr A Wardknott
• Safeguarding Governor – Mr Reg Edwardson
• Parents and Carers – Ms Carol Blatchford
• Parent Support Adviser – Jessica Crabtree
• The school will monitor the impact of the policy using:
• Logs of reported incidents
• SWGfL monitoring logs of internet activity (including sites visited)
• Internal monitoring data for network activity (AWK pricing auditing software)
• Surveys / questionnaires of
• pupils (CEOP ThinkUknow survey)
• parents / carers
• staff

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/ carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.
The school will deal with such incidents within this policy and associated behaviour, safeguarding and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

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 / Governors Sub Committee* receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body (Safeguarding Co-ordinator) 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
• regular monitoring of e-safety incident logs
• regular monitoring of filtering / change control logs
• reporting to relevant Governors committee / meeting

Headteacher and Senior Leaders:

• 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 Co-ordinator
• The Headteacher / Senior Leaders 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, as relevant

• The Headteacher / Senior Leaders 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 Leadership Team will receive regular monitoring reports from the E-Safety Coordinator
• The Headteacher and another member of the Senior Leadership 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. (see SWGfL flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures)

E-Safety Coordinator:

• leads the e-safety team
• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
• ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
• provides training and advice for staff
• liaises with the Local Authority
• liaises with school ICT technical staff
• 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 Leadership Team

ICT Technician 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 the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
• that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
• SWGfL is informed of issues relating to the filtering applied by the Grid
• the school's filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix "Filtering Policy Template" for good practice document)
• that he 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 and email is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Co-ordinator, Headteacher, ICT Co-ordinator or Class teacher for investigation
• that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff (including Supply Teachers and Student Teachers)

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 the school Staff Acceptable Use Policy (AUP) – see Appendix A
• they report any suspected misuse or problem to the E-Safety Co-ordinator, Headteacher, ICT Co-ordinator or ICT Technician for investigation.
• digital communications with students / pupils (email / Virtual Learning Environment (VLE) /voice) should be on a professional level and only carried out using official school systems
• e-safety issues are embedded in all aspects of the curriculum and other school activities

• pupils understand and are aware of e-safety issues and follow the acceptable use policy
• pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
• 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, when appropriate 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

Designated person for child protection / Child Protection Officer

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
(Note: it is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop. Some schools may choose to combine the role of Child Protection Officer and E-Safety

E-Safety Team

Members of the E-safety team will assist the E-Safety Coordinator with:
• the production / review / monitoring of the school e-safety policy / documents.
• the production / review / monitoring of the school filtering policy (if the school chooses to have one)

Pupils:

• are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. (N.B. at KS1 it would be expected that parents / carers would sign on behalf of the pupils)
• have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
• need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
• will be expected to know and understand 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 parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:
• endorsing (by signature) the Student / Pupil Acceptable Use Policy
• accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

Community Users
Community Users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign the Staff and Community User AUP before being provided with access to school systems.

Policy Statements
Education – pupils
Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of 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/PSHE/literacy 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.
• Pupils should be taught in all lessons to be critically aware of the material/content they access online and be guided to validate the accuracy of information
• Pupils should be helped to understand the need for the pupil Acceptable Internet Use Statement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
• 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,
• Parents evenings
• Reference to the SWGfL website

Education & Training – Staff
It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.
• The school will ensure that all staff are up to date with e-safety procedures. Training will be made available as and when appropriate.

Technical – infrastructure / equipment, filtering and monitoring
The school will be responsible for ensuring that the school infrastructure / 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 the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
• There will be regular reviews and audits of the safety and security of school ICT systems
• Servers, wireless systems and cabling must be securely located and physical access restricted to ENTS
• All users will have clearly defined access rights to school ICT systems.

• All users (at KS2 and above) will be provided with a username and password by the ICT Technician who will keep an up to date record of users and their usernames. Users will be required to change their password every term.
• The "master / administrator" passwords for the school ICT system, used by the Network Manager / Technician will also be available to the Headteacher and ICT Co-coordinator and kept in a secure place
• Users will be made responsible for the security of their username and password and 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.
• The school maintains and supports the managed filtering service provided by SWGFL
• In the event of the Network Manager / IT technician needing to switch off the filtering for any reason, or for any user, this must be logged. Such actions shall be reviewed regularly by the E-Safety Committee
• The IT Technician will 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, routers, wireless systems and 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" (e.g. trainee teachers, visitors) onto the school system.
• In the AUP we have a statement "Inappropriate private use of school systems is not permitted"
• An agreed policy is in place (to be described) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices. (see School Personal Data Policy Template in the appendix for further detail)
• 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.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and 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 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 on social networking sites
• Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
• Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:
• Fairly and lawfully processed
• Processed for limited purposes
• Adequate, relevant and not excessive
• Accurate
• Kept no longer than is necessary
• Processed in accordance with the data subject's rights

• Secure
• Only transferred to others with adequate protection.
Staff must ensure that wherever possible they:
• At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
• Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
• Transfer data using encryption and secure password protected devices. When personal data is stored on any portable computer system, USB stick or any other removable media, wherever possible:
• the data must be encrypted and password protected
• the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
• the device must offer approved virus and malware checking software
• the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete When using communication technologies the school considers the following as good practice:
• The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with pupils and parents
• Users need to be aware that email communications may be monitored
• Users must immediately report, to the nominated person – in accordance with the school policy, 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 pupils or parents/carers must be professional in tone and content.

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 i.e.
• Child sexual abuse images
• Adult material which potentially breaches the Obscene Publications Act
• Criminally racist material
• Other criminal conduct, activity or materials
The SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

Acknowledgements

In order to produce this policy we have referred to the SWGFL model School e-safety policy template (2009).
Approved by
Full Governing Body Date 28th June 2016 signed ……. Chair of Governors

Review date: ……June 2017…….

Appendix A

Staff, Governor and Visitor ICT Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers 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. 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 online safety in my work with young people.

Staff, Governor and Visitor
Acceptable Use Agreement/Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

Professional Use: I will only use the school's email/internet/Intranet/Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Headteacher or Governing Body.

Security: I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

Communications: I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

My Personal Details: I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other social media link, to pupils.

E-mail: I will only use the approved, secure e-mail system for any school business.

Other People's Personal Data: I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick.

Hardware/Software: I will not install any hardware or software without permission of the school's IT technician.

Inappropriate Material: I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

Photographs: Images of pupils and /or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member.

Distribution of Images: Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Headteacher.

Online Safety: I will support the school approach to online safety and not upload or add any images, video, sounds, or text linked to or associated with the school or its community.

Social Media: I will not use social networking applications in work time for personal use, unless permission has been given by the Headteacher. All proposals for using social networking applications as part of school service (whether they are hosted by the school or by a third party) must be approved by the Headteacher first.

Monitoring Use: I understand that all my use of the internet and intranet can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.

Copyright: I will respect copyright and intellectual property rights (including video and music copyright).

Online Activity: I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

E-Safety: I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

Electronic Devices: I will not use personal electronic devices, including smart phones, smart watches & smart eyewear, in public areas of the school between the hours of 8.30 am and 3.30 pm, except in the staff room and staff study. (Unless the use of which is essential to the running of the school e.g. The Site Manager.)

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. I understand this forms part of the terms and conditions set out in my contract of employment and I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Signature_____ Date_____

Full Name_____(Printed)

Job Title/Role Within School_____