WILDRIDINGS PRIMARY SCHOOL
e-Safety Policy

		Signature	Date
Headteacher	**Mr Simon Cope**		
On behalf of the Governing Body	**Mrs Sarah Hey**		

Version	
Reviewed by	Jason Francis
Approved by FGB	18th January 2018
Next Review	December 2020

1. Introduction

1.1 Introduction to this policy

This policy incorporates the e-safety policy and ICT/Computing policy, and relates to other policies including those for: Safeguarding, Behaviour, Anti-bullying, English & Mathematics Policy, Teaching and Learning Policy and guidance on Personal, Social, Health and Emotional Education (PSHE).

Our e-safety policy builds on the local discussions around e-safety and safeguarding, Bracknell Forest Borough Council's advice and recommendations, and government guidance. It has been agreed by the SLT and approved by governors and will be reviewed annually.

This policy should be adhered to when using any technology in school, including all devices that connect to the internet for both pupil and staff including but not limited to laptops, iPads, cameras and mobile devices.

1.2 Points of contact

Wildridings' first point of contact for e-safety is:
Simon Cope (Head Teacher and Lead Safeguarding Officer)

Support provided by:
Anna Cook (Deputy Lead), Chrissy Wort, Fran Tillman (Family Support Advisor) Jo Bond (Family Support Advisor) and Jason Francis (Computing Subject Co-ordinator)

1.3 Safeguarding Team

The safeguarding team is formed of a group of people who are responsible for:

- Developing and promoting the e-safety vision to all stakeholders and supporting them in their understanding of the issues
- Development of an e-safe culture
- Support in the escalation of e-safety incidents
- Receiving and reviewing e-safety incident logs
- Reviewing and updating e-safety policies and procedures annually

2. Importance of the internet and electronics

The use of technology and the internet is a quintessential aspect of 21st century life whereby it is incorporated into everything from day-to-day social interactivity, education and business. The school has a duty to its pupils to educate and inform them how to engage with technology and the virtual world effectively, enjoyably and, most importantly, safely.

2.1 The purpose of adults using the internet and electronic device in school is to:

- Support the professional work of staff
- Support the school's assessment process
- Enhance the school's management functions and administration systems
- Enable effective communication between the school, parents and outside agencies
- Support professional development for staff through access to national developments, educational materials and effective curriculum practice
- Improve access to technical support, including remote management of networks and automatic system updates
- Exchange curriculum and administrative data with Bracknell Forest Borough Council and the Department for Education (DfE).

2.2 By teaching children about the use of the internet and electronics, the school aims to:

- Raise educational standards
- Promote pupil achievement
- Develop responsible and mature approaches to internet use
- Enable users to evaluate internet information effectively
- Enable users to take care of their own safety and security.

3. Risks and risk management

Similar to other obtainable media, material available through viewing and/or downloading using the Internet may be unsuitable for pupils to access. In light of this, the school will always take all reasonable precautions to ensure the materials and resources that pupils experience when using technology within school, whether online or offline, is appropriate. In spite of this effort, due to the large scale and constant changing of the Internet and its online trends, there is no way to 100% guarantee that unsuitable material will never make an appearance on school devices. Neither the school nor Bracknell Forest County Council can accept liability for any such material being access, or any consequences that stems from accessing the Internet.

3.1 The school will manage risk through:

- A comprehensive, agreed and implemented e-safety policy
- A secure, filtered broadband network managed by Exceedia
- A school network that complies with the National Education Network standards and specifications
- Education for responsible computing use by staff and pupils, including protocols for staff and children on dealing with inappropriate content

3.2 Reviewing risk procedure and expectations

Methods to identify, assess and minimise risks will be reviewed regularly. For example:

- The SLT and safeguarding team will ensure that the e-safety policy is implemented and complied with via the guidelines found in the e-safety policy, Acceptable Usage Policies (see appendices), staff training and regular checks
- The use of computer systems without permission, or for inappropriate purposes, could constitute a criminal offence under the Computer Misuse Act 1990
- Access is strictly forbidden to any websites that involve radicalisation, pornography, violence, racism, gambling or financial scams.

3.3 Risk management: filtering

- The school will work in partnership with parents/carers, the LA and the Internet Service Provider (ISP) [Exceedia] to ensure systems to protect pupils are regularly reviewed and improved
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the safeguarding team
- Any material that the school believes is illegal will be referred to the Internet Watch Foundation (www.iwf.org.uk)
- The Computing Subject Co-ordinator, with guidance from the LA, will ensure that monthly checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate. The filtering strategy will be selected to suit the age and curriculum requirements of the pupils

3.4 Risk management: system security

It is important to review the security of the whole system, from user practice to ISP:

- The school computing systems will be reviewed regularly with regard to security
- Virus/Malware protection will be installed and updated regularly
- Personal data relating to pupils may not be sent from or to personal e-mail accounts. Instead, all staff must use secured school user email accounts to send data over the internet
- Portable media such as memory sticks and portable hard drives may not be brought into school without specific permission. It will be the user's responsibility to ensure that a virus/malware check is conducted if they deem it necessary.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or any e-mail attachments
- Files held on the school's network will be regularly checked by the Computing Subject Co-ordinator to ensure that users are following the protocols outlined in the relevant guidance
- Workstations and laptops will be secure from casual mistakes by the user
- The network manager [Exceedia] will ensure that the system has the capacity to take increased traffic caused by internet use
- All users must act in accordance with their Acceptable Use Policy or the guidelines within the e-safety policy
- Good password practice is encouraged, including logout after use and not giving passwords to others
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act.

3.5 Internet access

Internet use is a key part of the curriculum and is an entitlement for all responsible and mature users. Government guidance suggests that, in primary schools, all pupils are granted internet access as a class group with full supervision of all pupil use:

- Parents/carers will be informed that pupils will be provided with supervised internet access
- Staff, student teachers or other staff undertaking placements at the school will sign an Acceptable Use Policy (Appendix A) before using the internet on any school ICT resource
- The school will keep an up-to-date record of all staff and pupils who are granted internet access
- At Foundation Stage and Key Stage 1, access to the internet will be by adult demonstration, with supervised access to specific, approved online materials.

- Parents are required to give permission for their child to use the internet within school and support the school in e-safety when their child is at home (Appendix B)

3.6 Risk management: e-mail

The use of email is a fundamental means of communication in today's society and is beneficial to an educational establishment for both direct contact with registered and approved clientele as well as understanding and learning of modern communicative methods. However, an email system that is not properly organised, utilised or monitored can implement a number of risks such as, but not limited to: transmission of malware and viruses, contact with inappropriate content, cyber bullying. Therefore, the usage of email within school must be carried out with appropriate safety, security and care including these guidelines:

- Pupils may only use approved e-mail accounts on any of the school's ICT systems and devices
- Whole-class or group e-mail addresses should be used, unless discussed with the Computing Subject Co-ordinator prior to the set-up of singular e-mail addresses
- Pupils are taught that they should immediately tell an adult if they receive offensive e-mail
- The forwarding of chain letters is not permitted
- Personal emails or messaging between staff and pupils should not take place
- Pupils must not reveal details about themselves, others or the school in e-mail communication or via a personal web space, such as address or telephone number, or arrange to meet anyone
- E-mail by staff that is sent to an external organisation should be written carefully and authorisation sought if considered necessary. Staff are responsible for sending their own e-emails which uphold the polices of the school
- Staff must use secured school user accounts to send any data about pupils over the internet. This includes assessment data, reports, IEP's, SEND referral information and information relating to the personal circumstances of pupils or their families.

3.7 Risk management: school website

Websites can celebrate pupils' work, promote the school and publish resources for pupil use. Whilst there are many ways to obtain information about schools and pupils, a school's website can be accessed publicly. For security purposes, the following will be considered:

- The point of contact on the website should be the school address, school e-mail and telephone number
- he home contact details of staff, governors and pupils will not be published
- Website photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified
- Pupils' full names will not be used in association with photographs. However, it is acceptable to use first names. No child will be clearly identified with a name and a year group, unless as part of a group (e.g. Year 5/6 Football Squad: Child [insert name])
- Parents will be informed about the digital image procedures
- The Computing Subject Co-ordinator will take overall editorial responsibility and ensure that content is accurate and appropriate
- The website should comply with the school's guidelines for publications
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce it has been obtained.

3.8 Risk management: photographic, video and audio technology

The use of digital imaging technology, both visual and auditory; photography and video, has proven to be an excellent resource when engaging and enhancing pupils' learning through both their experience of it and through hands-on practicality. Examples such as video/audio recording (e.g.

podcasting, digital video/cameras). However, prevention of misuse and user protection must be held in consideration including the following:

- The downloading of audio or video files is only permitted when being downloaded onto school computing hardware (e.g. laptops), unless the user has gained prior permission from the network manager/Computing Subject Co-ordinator
- Audio or video files may only be downloaded if they relate directly to the current educational task being undertaken
- Pupils should always seek the permission of their teacher before making digital image or audio recordings within school
- Staff, student teachers or other staff undertaking placements at the school will sign the Acceptable Use Policy for staff (Appendix A)
- Staff may take digital images to support school trips and curriculum activities, including assessment and record keeping
- Staff will not use personal digital cameras or video cameras to take digital images of any pupils without written permission from a member of the SLT (Appendix C) for a specific event or activity (e.g. recording the summer production or attending a sporting event with a professional camera).
- If staff use personal devices, they are required to delete any school-related photos as soon as they are uploaded to school hardware (e.g. laptops/network). If images cannot be removed from the device for any reason, it must be kept at school until such a time as it is possible to download the media onto a school network
- Staff may use and store digital images and audio recordings needed for professional purposes on school laptops and computers off the premises. However, images must be free of any information that would enable identification and tracking of children (e.g. adding names to photographs)
- It is not appropriate to use digital image or audio devices in situations/places where a child may be captured in an unsuitable state (e.g. in the toilet, whilst changing for P.E., in changing rooms etc.)
- Care should be taken when capturing digital images to ensure that all pupils are appropriately dressed
- Staff and pupils are aware that their use of technology may be monitored for safety
- Any images of children used in school training and promotional materials (e.g. websites and prospectus) will not include full names of the children
- Parents/carers will be informed about the school's digital image procedures and given the option to refuse consent for their child to appear in digital images taken by the school (Appendix B). It is the responsibility of parents/carers to inform the school, in writing, if they wish to change their decision
- The school will keep an up-to-date record of all pupils who do not have parental consent to appear in digital images
- All staff must sign the Acceptable Usage Policy before using any school computing resource
- The school's policy regarding digital images will be reviewed regularly in consultation with the LA and Local Safeguarding Children Boards, with regard to security
- Parent/carers are permitted to take pictures of their own child/children at class assemblies, school productions and school sports events. However, this privilege could be withdrawn if deemed to be inappropriate. Please also note section 3.11's guidance on posting photos on social media.

3.9 Risk management: social networking and personal publishing (pupils and parents)

The use of personal online spaces and social media has enabled a greater and more efficient means of communication for various purposes. These may be used in an educational environment to help

promote, discuss and educate subjects and the school to further enhance learning experiences and optimise communicating with approved and registered personnel linked to the school. Unfortunately, with the broad and open nature of social media, unmoderated content can be made public which may lead to a breach in e-safety and safeguarding protocols e.g. cyber bullying, radicalisation, racist, negative imagery etc. To protect against this potential risk, the school will implement the following:

- Newsgroups or other open forums will not be made available to pupils unless an educational requirement for their use has been demonstrated
- The school will block access to social networking sites for pupils, although staff may use these for educational purposes
    - With regard to social networking, pupils will be permitted to access and use school accounts if supervised by a member of staff, who takes full responsibility for the content seen and posted
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include: real name, address, mobile or landline phone numbers, school attended, instant messenger and e-mail addresses, full names of friends, and specific interests etc.
- Pupils should be advised not to place personal photos on any social network space
- Pupils should be advised not to publish specific and detailed private thoughts about themselves or others
- Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing information once published
- Pupils should be advised on security of personal internet spaces and encouraged to set passwords, invite known friends only and deny access to unknown individuals
- Teachers, parents/carers and pupils should be aware that bullying can take place through social networking and messaging and taught how to address these issues
- Advice regarding the use of forums, social networking sites and messaging facilities will be provided for parents/carers i.e. through the school website, newsletters etc.

As many children now have access to tablets and other mobile devices at home, there may be times when social communication such as Facebook, Whatsapp or Snapchat may lead to cyber bullying. Although this may occur outside of school, Wildridings Primary School and Wildridings Nursery will support parents and carers with issues, both by investigating incidents and by promoting a good understanding of potential issues. This will be done by:

- Teaching children about cyber bullying and e-safety as part of Computing/PSHE lessons
- Providing families with information on keeping children safe when using social communication
- Supporting families through issues by working with all parties and investigating, where appropriate.

3.10 Risk management: social networking and personal publishing (staff)

Social media and their networks are growing massively in their popularity and are used by a range of people of varying ages. Despite this, teachers and teaching staff have an image of professionalism to uphold and this extends to the image and conduct perceived when online. Whilst the use of social media applications such as Facebook, Instagram, Twitter, Snapchat etc. is not prohibited, staff are to exercise appropriate caution when using these platforms. Therefore, the following suggestions have been made for safety purposes:

- Do not post personal information about yourself, e.g. address, phone number
- Never post any pictures of yourself or pupils at school on private accounts; this includes pictures of classrooms and the school grounds

- Use the privacy features provided on the site to restrict access of strangers and those who you have not specifically selected as 'friends' to your profile
- Adjust your privacy settings so only your online 'friends' are able to view your photos and any photos in which you are 'tagged'
- Do not discuss pupils, parents, colleagues or the school itself on social networking sites
- Use a strong password (i.e. more than 8 characters made up from a mixture of letters, numbers and other symbols) and change it regularly
- Consider the posts you make carefully, and the impact that these may have on you, the school and its children. Some comments made online can be used in criminal and/or disciplinary cases.

At Wildridings Primary School and Wildridings Nursery, staff members may also be parents of children in our school and community. Therefore, it is very difficult to enforce the statement "do not accept or initiate any friend requests with pupils or parents associated with the school". However, it is suggested that staff should:

- Strongly consider their public image
- Strongly consider friend requests from children, even if they are family friends:
    - Are the children of a legal age to be on that social media site?
    - What of my profile could be seen/screenshot?
    - Is this creating a conflict between my professional and home boundaries?
- Remember that parents can and may share your content, or show others, if you are friends with them on social network sites
- Be aware of local groups and sites and what they post on open forums/platforms
- Consider the language used in posts
- Consider the impact of their comments/views/shared pictures or videos on the school or individuals
- Be aware of their role as an educator and role model, ensuring grammar is of a high standard.

3.11 Risk management: mobile phones in school

Mobile phones are an inevitable and important part of adult life, with most – if not all – staff members, visitors, parents and contractors bringing a mobile phone on site. The following restrictions, rules and guidelines have been set out to safeguard the children in our school:

For children:

- Mobile phones will not be used during lessons or formal school time unless, due to exceptional circumstances, specific permission has been granted to the family, in which case the phone will be kept by the class teacher during school hours
- Pupils in Years 5 and 6 only may bring a mobile phone to school. The phone must be turned off or placed on 'silent mode' and kept at the school's reception desk. The school governors and staff recognise that many Year 5 and 6 pupils are becoming independent in their travel to and from school, and wish to formally support parents in their children's safeguarding
- However, the school takes no responsibility for any personal property (including mobile phones) brought onto the school premises
- Mobile phones that are used in school without permission may be confiscated by a staff member. If this occurs, the parents will be notified via a phone call, face-to-face meeting or letter

For staff:

- Mobile phones should not be visible or used during lessons or times when children are present
- On trips and activities, staff are permitted to communicate via personal mobile phones but may not take pictures of pupils using personal mobile phones or devices. Pictures may be taken using registered school devices to be uploaded to school network drives at the earliest convenience
- Staff should ensure family members have the school's main contact number, so that they are able to reach staff members in an emergency, as opposed to using personal mobile devices
- Staff will not use mobile phones to take digital media of any pupils, at any time. Staff may, however, use tablets, school cameras/video cameras

All volunteers, visitors, governors and contractors are expected to follow our mobile phone policy, as it relates to staff whilst on the premises. On arrival, such visitors will be informed of our expectations around the use of mobile phones. Volunteers, contractors and other visitors will have the key points of the e-safety policy (e.g. regarding mobile phones) explained to them in the form of signs and verbal explanation upon arrival.

3.12 Risk management: mobile phone use on residential and out of school activities/events

We recognise that mobile phones provide a useful means of communication on off-site activities. However, staff should ensure that:

- Personal mobile use on these occasions is appropriate and professional (and will never include taking photographs of children)
- Personal mobile phones should not be used to make contact with parents during school trips. All relevant communications should be made via the school office, or via the school mobile phone/s
- Where parents are accompanying children and staff on trips/events (in which they hold a position of responsibility, such as being assigned to a group for a school trip to a museum), they are informed not to make contact with other parents (via calls, text, email or social networking) during the trip or use their phone to take photographs of children
- On trips/events, when parents are accompanying children and staff, parents will be made aware of the expectations with regard to the above points, both in writing and verbally

4. Education in e-safety

Whilst managing information systems forms an essential part of protecting internet users, empowering learners to develop safe and responsible online behaviours is a priority if they are to be protected whenever and wherever they go online.

4.1 What the school has in place:

- A unit of work giving direct e-safety teaching and instruction is included in the PSHE and Computing programme of study for KS1 and KS2, covering both home and school internet use
- Pupils will be taught what internet use is acceptable and what is not (e.g. in relation to cyber-bullying and accessing inappropriate material)
- Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening
- In Foundation Stage and KS1, younger pupils may be guided to appropriate websites and taught search skills within restricted online environments

- In Key Stage 2, pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Pupils will be taught to avoid hardware becoming infected with and transmitting computer viruses or malware
- Pupils will be taught to keep personal information private to protect them from online predators and identify theft
- Pupils will be taught how to report concerns and contact with inappropriate material
- Children will be aware of their Acceptable Use Policy and this will be displayed nearby all relevant technology (Appendix B).

4.2 Respecting Copyright

In most instances, pupils will be judging appropriate material but will need to select relevant sections. They will be helped to understand that unselective copying is of little value and the reproduction of copyright materials can be a criminal offence, equivalent to theft.

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work
- The school will ensure that the copying and subsequent use of internet-derived materials by staff and pupils complies with copyright law.

5. E-safety incidents

Despite the comprehensive e-safety measures in place, there may still be occasions when e-safety incidents occur. As such, there are clear guidelines for responding to e-safety incidents, such as cyber-bullying, transmission of viruses/malware, security breaches and access to inappropriate materials.

5.1 Accidental access to inappropriate content

- Inappropriate content is defined as any access to materials which contain violent, harmful or sexual content and/or reference to radicalisation, cultural, racial or homophobic discrimination
- All incidents of accidental access to inappropriate materials are immediately reported to the named safeguarding teams using the Incident Report Form and selecting the “E-safety” tick box to highlight this type of concern (Appendix D). The site URL is recorded for inclusion in the list of blocked sites
- Any access to inappropriate material is formally documented in school and then passed on to the school’s Internet Service Provider (ISP) to investigate further
- Any material that the school believes is illegal will be referred to the Internet Watch Foundation (www.iwf.org.uk)
- Filtering is regularly checked by network manager, Internet Service Provider (ISP) [Exceedia] and South East Grid for Learning (SEGfL). ISP monitor standards by producing reports of blocked sites and internet usage
- Any inappropriate content accessed whilst using resources posted on the school’s website must be reported to the school, and all links will be removed.

5.2 Suspected breach of the school's Acceptable Use Policy (AUP)

The school may exercise its right to monitor the use of the school's computer systems. This includes access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes, or for storing unauthorised or unlawful text, imagery or sound.

5.3 Deliberate breach of the school's Acceptable Use Policy (AUP)

- All e-safety incidents are promptly reported to the named safeguarding team. The incident will then be recorded in the Incident Report Sheet (see Appendix D) and be escalated following the school's E-safety Incident Escalation Flowchart (see Appendix E)
- The incident log will be reviewed termly by the safeguarding team
- All incidents of misuse (from staff or pupils) will be promptly reported to the Head Teacher or safeguarding team
- Different e-safety incidents will require different responses, depending on the nature of the event. Sanctions may include:
    - Disciplinary action
    - Interview/counselling by Head Teacher or appropriate agency
    - Informing parents/carers
    - Removal of internet or computer access for a specified period
    - Involvement of outside agencies specified by the Escalation Flowchart
- Incidents of cyber-bullying will be dealt with in line with the school's Anti-bullying policy
- There may be occasions when the police must be contacted. Early contact should be made to establish the legal position and discuss strategies. Advice sought should include how best to preserve any possible evidence
- Parents/carers and pupils will need to work in partnership with staff to resolve issues

6. Involvement of the school community

E-safety is primarily a safeguarding issue, so anyone with responsibility for the welfare of children and young people needs to be involved, including the children themselves.

6.1 Involvement of staff

- Staff will have access to the e-safety policy and will sign an Acceptable Usage Policy to agree with the rules, restrictions and guidelines
- All new staff will be provided with a copy of this policy on joining the school and will be taken through the key parts of the policy as part of their induction
- All teaching and support staff will receive training in e-safety issues as required and are expected to take personal responsibility for their professional conduct and development in this area
- Teachers will be involved in delivering age appropriate e-safety instruction to their pupils
- All staff are aware of their responsibilities to report any misuse or suspected misuse of the ICT systems in school
    - Report any known misuse of technology and e-safety incidents (e.g. the viewing of inappropriate material or cyber-bullying) to the safeguarding team. This information will then be passed on through the appropriate channels (see e-safety policy, Appendix E)

- Report any failings in network filters (e.g. inappropriate material being accessed) to the Computing Subject Co-ordinator using the Incident Record Sheet and reported to the safeguarding team

- Staff understand that, in order to safeguard children, the following statements apply:
  - Wildridings Primary School and Wildridings Nursery reserves the right to monitor the network and examine or delete any files that may be held to ensure the safety of all staff and children
  - The network is the property of Wildridings Primary School and staff agree that their internet activity must be appropriate with their professional role or the children's education
  - Deliberate misuse of the network, electronic devices and ICT systems may result in disciplinary action.

6.2 Involvement of pupils

- All pupils are made aware of their rights and responsibilities when using ICT systems through the Pupils' Acceptable Use Policy and posters (see Appendix C)
- The Pupils' Acceptable Use Policy is drawn up in consultation with pupils through class discussion and School Council
- The Pupils' Acceptable Use Policy is posted in all rooms where computers are used and children's attention drawn to relevant items during teaching
- Instruction in responsible and safe use should precede internet access and be revisited regularly through the taught Computing curriculum
- Modules giving direct e-safety teaching and instruction are included in the PSHE or Computing programme of study for KS1 and KS2, covering both home and school internet use
- Pupils will be informed that their internet use will be monitored
- School Council have contributed to and agreed upon the Acceptable Usage Policies to encourage safe practices within the home.

6.3 Involvement of parents

Unless parents and carers are aware of the dangers, pupils may have unrestricted access to the internet at home. Steps have been taken to improve parents'/carers' understanding of the risks of internet use and develop the use of safe practices within the home as well as at school.

- The Acceptable Use of Internet and Digital Images Consent Form (Appendix B) requires parents to give permission for their child to use the internet within school, and to support the school in e-safety when their child is at home. This is done via the Home School Agreement
- A partnership approach with parents/carers will be encouraged to ensure a shared understanding of e-safety advice between staff, pupils and parents/carers. This may include training events, demonstrations, information leaflets and suggestions for safe internet use at home
- E-safety issues will be handled sensitively to inform parents without undue alarm
- Advice on filtering systems will be made available to parents
- Access to and advice on educational activities, appropriate leisure activities, and advice on responsible use of the internet will be offered to parents through the school website.

6.4 Involvement of community

Internet access is available in many situations in the local community, including after-school child care facilities and clubs/organisations such as Cubs/Brownies. Ideally, young people would encounter a consistent policy to internet use wherever they are. Although this may not always be possible, attempts will be made to communicate our e-safety vision with community partners.

- The school will liaise with organisations associated with the school to establish a common approach to e-safety
- The school will be sensitive to internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice
- Any organisation using the school's computing systems and network will be expected to comply with the e-safety policy
- All staff and children using the school's computing systems will be required to understand and sign an Acceptable Use Policy, appropriate to their age, role and computing use.

Contents of Appendices

*** Please note that Appendices C and D can be found in the Home-School Agreement, which is sent out to parents yearly. This is where these agreements are made.**

*** All appendices that are required for staff and for school use should be copied into official, headed document paper and printed/sent out. Do not print directly from this policy.**

Staff and Volunteers
Acceptable Use Policy
2017-2018

Next Review Due Summer 2018

For the purpose of this policy, the 'Head Teacher' refers to Mr S. Cope, Head teacher of Wildridings Primary School. Jason Francis is the ICT Coordinator.

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 technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion and promote creativity, promoting effective learning. They also bring opportunities for staff to be more creative and productive in their work.

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be safe and responsible users of the internet and other digital technologies.
- That school ICT systems and users are protected from accidental or deliberate misuse.
- The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work and improve opportunities for learners 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 minimise the risk to my safety or to the safety and security of the ICT systems and other users. 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 its ICT systems including email and other digital communications technologies.
- I understand that this agreement also apply to use of school ICT systems out of school (e.g. laptops, email, VLE etc.).
- 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 keep my usernames and passwords private and will not try to use anyone else's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, to the appropriate person in school.
- I will be professional in my communications and actions when using school ICT systems:
- I will not access, copy, delete or otherwise alter any other user's files, without their permission.
- I will communicate with others in a professional manner.
- I will ensure that when I take or publish images of pupils or parents/colleagues, I will do so with their permission and in accordance with the school's policy. I will not use my personal equipment to record these images, unless I have permission to do so.
- Where these images are published (e.g. on the school website) it will not be possible to identify pupils by name, or other personal information.

- I will only communicate with pupils and parents / carers using official school systems and in a professional manner. I will not share any personal information with a pupil (including personal phone numbers or email address). Nor will I request or respond to any personal information from a young person unless it is appropriate as part of my professional role.
- 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:

- When I use my personal hand held / external devices in school (PDAs /laptops / mobile phones / USB devices etc.), I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I will also follow any additional rules set by the school about such use. I will ensure that when connecting these devices to school ICT systems, they are protected by up to date anti-virus software and are free from viruses.
- 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 try to upload, download or access any material which is illegal or inappropriate or may cause harm or distress to others (e.g. child sexual abuse images, criminally racist material, adult pornography (etc.).
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems intended to prevent access to such materials.

Unless I have permission, I will not try 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 install or attempt to install programmes of any type on school systems, nor will I try to alter computer settings, unless this has been authorised by Jason Francis the school ICT Technical Support coordinator.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy.
- Where personal data is electronically transferred outside the secure school network, it must be encrypted.
- 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 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.

Signed …….. Print name…….

School……..

Wildridings Student / Pupil Acceptable Use Policy Agreement – for KS1 pupils

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers

- I will only use activities that a teacher or suitable adult has told or allowed me to use.

- I will take care of the computer and other equipment

- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

- I will tell a teacher or suitable adult if I see something that upsets me on the screen.

- I know that if I break the rules I might not be allowed to use a computer.

Name of student	
Class	
Signed by Parent on behalf of the pupil	
Date	

Wildridings Student / Pupil Acceptable Use Policy Agreement – for KS2 pupils

This is how we stay safe when we use computers:

- I understand that I am responsible for my own actions.
- I will use my knowledge of internet safety to guide me whenever and wherever I am online.
- I will only use the network, Internet and e-mail when a teacher has given permission.
- I will only access the network with the login and password I have been given and I will keep my password secret.
- I will not access other people's files without their permission.
- I understand that the school will check my computer files and monitor the internet sites I visit.
- I will respect copyright and not copy anyone's work and call it my own.
- I will not bring in software from outside school and try to use it on the school computers.
- I will only e-mail people I know, or a teacher has approved.
- I will be polite and responsible when sending e-mail and will not forward any chain letters.
- I will not give any personal details to anyone on the Internet or in any e-mail or arrange to meet anyone out of school.
- I will report any unpleasant material to a teacher immediately because this will help protect other pupils and myself.
- I will discuss internet safety issues with my parents or carers and uphold any rules for safe internet use in my home.
- I know that if I break the rules I might not be allowed to use a computer.
- If I bring my mobile phone to school I will make sure it is switched off and handed into reception.

Name of student	
Signed by the student	
Class	
Signed by Parent on behalf of the pupil	
Date	

PERMISSION FOR PHOTOGRAPHS

At Wildridings Primary School we take the issue of child safety very seriously, and this includes the use of images of pupils. Using images of pupils in school publications and on the school website can be motivating for the pupils involved and provide a good opportunity to promote the work of the school. However, schools have a duty of care towards pupils, which means that pupils must remain unidentifiable, reducing the risk of inappropriate contact, if images are used in this way.

I am writing to inform you of our policy on photographing pupils. We have updated the policy to take into account the growth in digital media and in order to ensure that we fulfil the requirements laid down by Bracknell Forest Borough Council.

We would ask that you read the attached policy and sign the 'Photographs Permission' slip below as soon as possible. We will use the returns in order to create a database, identifying the pupils for whom we have parental permission to photograph for the purposes defined.

Once signed, the agreement will stay in operation for the duration of the academic year. If you wish to change your response to the questions at any stage in the future, please inform us in writing so that we can update our records.

Parental Permission Form

1. **I give / I do not give* permission for my child..... to participate in any photograph or image relating to educational activities linked to Wildridings Primary School for use by the school or by local media.**

Signed:.....Parent/Carer Date: .....

2. I am / I am not* happy for my child's name to be used alongside photographs in the newspaper.
Signed:.....Parent/Carer Date: .....

3. **I agree that any photograph or video I take at a school event will be for personal, family use.**
4.

Signed:..... Parent/Carer Date: .....
*Please delete as appropriate**

Incident Record Sheet

Date:	**Time:**	**Childs name:**	**Class:**
Others involved:		**Form completed by:**	

Information received:
(actual information received, do not make judgements-please attach any related letters/notes)

General incident		**Racial**		**Physical**		**Online safety issue**	

Please tick

If required:

Childs name:	Childs name:	Childs name:	Childs name:
Signature:	Signature:	Signature:	Signature:

Any actions taken (please date actions):

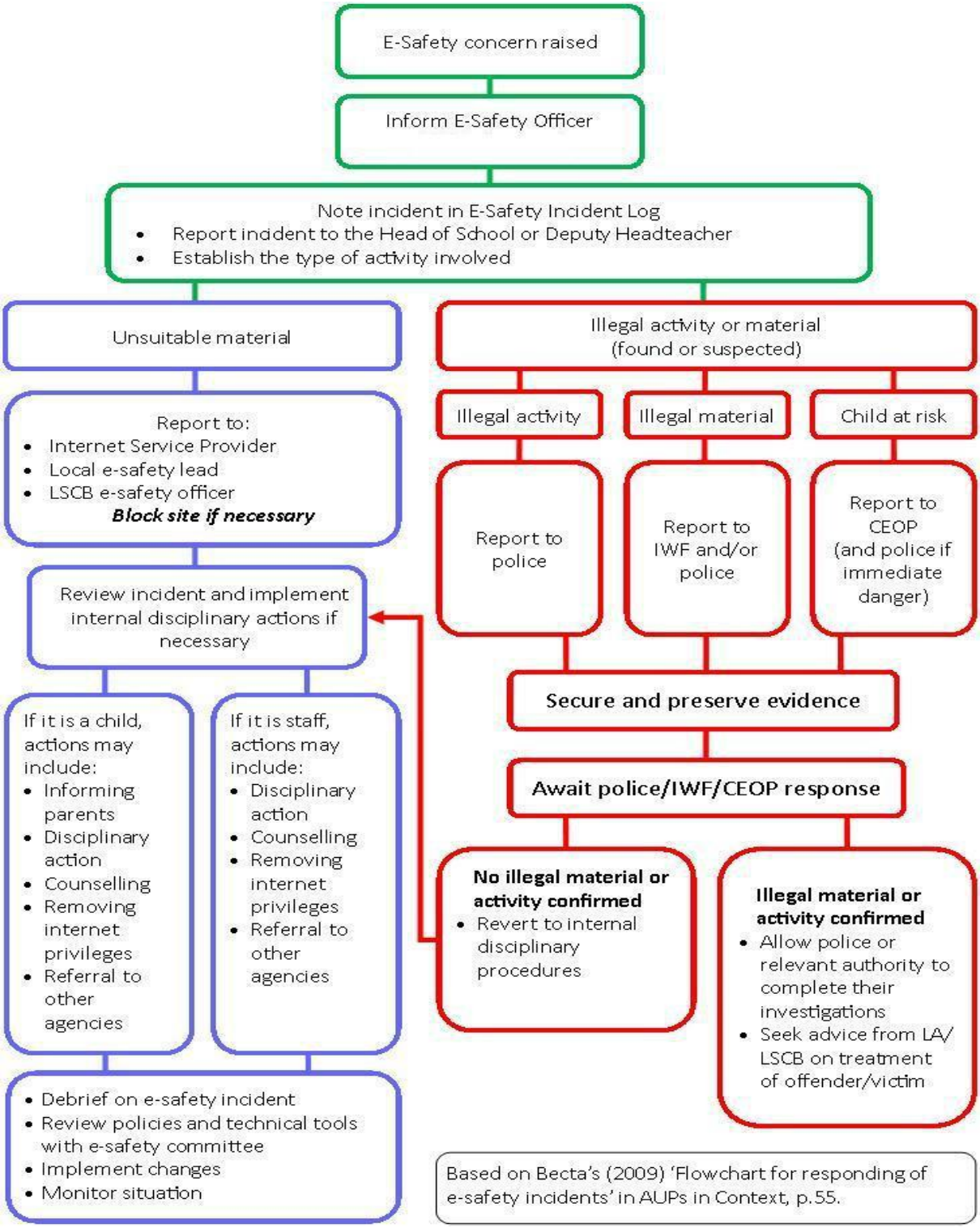
Copy of incident report must be given to the class teacher. Please tick below if the incident needs to be escalated.

Team Leader		Headteacher		Deputy Headteacher		FSA	

Parents phoned: Yes / No (Please circle)

REPORT TO BE FILED IN CHILD'S INCLUSION FOLDER

E-safety Incident Escalation Flowchart



Definitions: **LSCB: Local Safeguarding Children Board**
IWF: Internet Watch Foundation
CEOP: Child Exploitation and Online Protection Centre

Managing incidents support form

The Head of School/safeguarding team/safeguarding officer will ensure that an adult follows these procedures in the event of any misuse of the internet:

Has there been inappropriate contact?

1. Report to the organisation manager/e-safety lead/child protection officer
2. Advise the child, young person or vulnerable adult on how to terminate the communication, and how to save all evidence
3. Contact the parent(s)/carer(s)
4. Contact the police on 101
5. Log the incident
6. Identify support for the child, young person or vulnerable adult

Has someone been bullied?

1. Report to the organisation manager/e-safety lead/child protection officer
2. Advise the child, young person or vulnerable adult not to respond to the message
3. Refer to relevant policies including anti-bullying, e-safety and AUP and apply appropriate sanctions
4. Secure and preserve any evidence
5. Contact the parent(s)/carer(s)
6. Consider informing the police on 101, depending on the severity or nature of the offence
7. Log the incident
8. Identify support for the child, young person or vulnerable adult

Has someone made malicious/threatening comments? *(child/young person/vulnerable adult or organisation staff/volunteer)*

1. Report to the organisation manager/e-safety lead/child protection officer
2. Secure and preserve any evidence
3. In the case of offending web-based e-mails being received, capture/copy the 'header' info, if possible.
4. Inform and request that the comments are removed from the site/block the sender
5. Inform the police on 101 as appropriate
6. Log the incident
7. Identify support for the child, young person or vulnerable adult

Has an inappropriate/illegal website been viewed?

1. Report to the organisation manager/e-safety lead/child protection officer
2. If illegal, do not log off the computer and contact the police on 101
3. Record the website address as well as the date and time of access
4. If inappropriate, refer the child/young person/vulnerable adult to the AUP that was agreed and reinforce the message
5. Decide on the appropriate sanction
6. Inform the parent(s)/carer(s)
7. Contact the filtering software provider to notify them of the website
8. Log the incident
9. Identify support for the child, young person or vulnerable adult

Has an allegation been made against a member organisation staff/volunteer?

Child/Young People Organisation

In the case of the above, the Berkshire LSCB Child Protection Procedures should be referred to: http://proceduresonline.com/berks/.

All allegations should be reported to the organisation manager, police (101) and the Local Authority Designated Officer (LADO) (01344 352020), as appropriate.

Vulnerable Adult Organisation

In the case of the above, the Berkshire Safeguarding Adults Policy and Procedures should be referred to:
http://www.sabberkshirewest.co.uk/practitioners/berkshire-safeguarding-adults-policy-and-procedures/

All allegations should be reported to the organisation manager, police (101) and the Community Response and Re-enablement Team (01344 351500), as appropriate.

Further advice and guidance on inappropriate and illegal acts involving the internet and electronic communication technologies is shown below.

Children and Young People

To discuss an e-safety concern involving a child or young person, please contact Children's Social Care & Duty Team 01344 352020

Vulnerable Adults

To discuss an e-safety concern involving a vulnerable adult, please contact Adult Social Care and Health Community Response and Re-enablement Team on 01344 352000

For professional advice, contact the UK Safer Internet Centre's Helpline on helpline@saferinternet.org.uk or 0844 381 4772.

To request an e-safety presentation for parents/carers or for children, young people and vulnerable adults, please contact Childnet on kidsmart@childnet.com

A copy of this form can be found in a separate document.

Permission to use personal digital equipment

This is form should be used for each event or activity, and will be reviewed annually.

Staff member's/visitor's name								
Personal device requested								
Length of time requested	From	dd	mm	yy	To	dd	m	yy
Reason for request (e.g. event name)								

I, the above staff member/vistor, request to use a personal device (noted above) for a school activity. I understand the restrictions and requirements for using my personal device (e.g. sending the photos as soon as the event is done and deleting media afterwards).

I understand that the E-safety Policy details the rules, restrictions and requirements for using a personal device. By signing the Acceptable Usage Policy, I have already agreed to uphold these rules.

I also understand that any breach of protocol may result in disciplinary action, and I also understand that, should a member of the e-safety committee request to check my device to ensure the photos have been deleted, I must adhere to this request.

Signed (above named staff member/visitor)	

Decision

SLT Member's name								
Request granted?	Yes				No			
Length of time permission is granted	From	dd	mm	yy	To	dd	m	yy
SLT Member's signature								

This completed form is to be given to the ICT Technician to be filed.