E-Safety and Computing Policy

Date reviewed by School	December 2018		
Date ratified by FGB	29th January 2019	**Version ratified**	V5
Date for next review	Spring 2022		

	Print name	Signature	Date
On behalf of the Head Teacher	**Mr P Sherwood** Head Teacher	[signed in meeting]	29 / 01 / 2019
On behalf of the Governing Body	**Mrs J Steadman** Chair of Governors	[signed in meeting]	29 / 01 / 2019

1 Introduction

1.1 Introduction to this policy

1.1.1 This policy incorporates the e-safety policy and ICT/Computing policy, and relates to other policies including those for Safeguarding, Behaviour and Anti-Bullying.

1.1.2 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 every three years.

1.1.3 This policy should be adhered to when using any technology in school, including all devices that connect to the internet, such as pupils' iPads and laptops, as well as staff laptops, iPads, cameras and video cameras.

1.2 Points of contact

- E-Safety Officer: Ruth Deacon (Deputy DSL)
- Support provided by: Alison Stone (IT Technician)

2 E-safety committee

2.1 The e-safety committee is formed of two or more people, holding the titles of e-safety officer, Head Teacher, Designated Safeguarding Officers and Safeguarding governor.

2.2 The e-safety committee is responsible for:

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

3 Risks and risk management

3.1 In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users only access appropriate material. However, due to the international scale and ever-changing nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school device. Neither the school nor Bracknell Forest Borough Council can accept liability for such material accessed, or any consequences of internet access.

3.2 The school will manage risk through:

- A comprehensive, agreed and implemented e-safety policy
- A secure, filtered broadband network
- A school network that complies with national standards and specifications
- Education for responsible computing use by staff and pupils, including protocols for staff and children on dealing with inappropriate content
- Certification of practice (i.e. holding Cyber Essentials certificate).

3.3 **Reviewing risk procedure and expectations**

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

- The SLT and e-safety officers 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 for compliance
- 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.

3.4 **Risk management: filtering**

- The school will work in partnership with parents/carers, the LA and the Internet Service Provider (ISP) 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 e-safety officers
- Any material that the school believes is illegal will be referred to the Internet Watch Foundation (www.iwf.org.uk)
- The IT Technician, 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
- Advice on filtering systems will be made available to parents. This is achieved by the IT Technician updating the school website with information on filtering.

3.5 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 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 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 check is conducted via the IT Technician before use, and they will be liable if not conducted
- 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 IT Technician to ensure that users are following the protocols outlined in the relevant guidance
- The network manager 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 (Appendix G), 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 2018 (DPA 2018).

3.6 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 IT resource
- The school will keep an up-to-date record of all staff and pupils who are granted internet access (the IT Technician)
- At EYFS 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, as part of data collection and consent requests, in line with DPA 2018.

3.7 Risk management: e-mail

3.7.1 The government encourages the use of email as an essential means of communication for both staff and pupils.

3.7.2 However, unmediated email access carries many risks such as cyber-bullying, transmission of viruses, contact with inappropriate material and identity theft. Therefore, use of e-mail in school must be carefully monitored to ensure safety and security.

- Pupils may only use approved e-mail accounts on the school system and laptops
- Whole-class or group e-mail addresses should be used, unless discussed with the Computing Subject Leader 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 email or messaging between staff and pupils should not take place
- Pupils must not reveal details of 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
- Email 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 emails which uphold the polices of the school
- Staff must use secure school user accounts to send any data about pupils over the internet. This includes assessment data, reports, IEPs, SEND referral information and information relating to the personal circumstances of pupils or their families.

3.8 Risk management: school website

3.8.1 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.

3.8.2 Publication of information should therefore be considered from a security viewpoint:

- The point of contact on the website should be the school address, school email and telephone number
- The 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 may be 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], Child [insert name] etc.)
- Parents will be informed about the digital image procedures
- The IT Technician will take overall editorial responsibility for the website 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.

3.9 Risk management: photographic, video and audio technology

3.9.1 Digital image technologies and audio recordings can be very powerful learning tools. It should be noted at that this point that 'digital images' refer to both digital photographs and digital videos. Video conferencing, audio recording (e.g. podcasting, digital video and digital cameras) may all be used in the classroom to enhance learning activities.

3.9.2 The following statements are included to prevent misuse and to protect users and subjects:

- 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/IT Technician
- 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 using a school device to support school trips and curriculum activities, including assessment and record keeping
- 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. 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
- The school's policy regarding digital images will be reviewed in consultation with the LA and Data Protection Officer (DPO), with regard to security
- Parents/carers are permitted to take pictures of their own child/children at class assemblies, school productions and school sports events. Please also note section 3.9.3's guidance on posting photos on social media.

3.9.3 Parents/carers should be mindful of posting on social media, and the impact it may have on students, staff, governors and other families. It is imperative that families within Uplands Primary School and Nursery are respectful and professional towards the school and its members of the community. For example, parents/carers should:

- Not make inflammatory remarks about Uplands, its staff, pupils or other family members. This can be a prosecutable offence
- Follow official communication channels if they require support/assistance
- Not mention any pupil by name in a photo attached to the school's social media accounts
- Avoid posting images and videos with other children in the media, as there may be children whose parent/carer does not wish them to be on social media
- Consider the role of friends who are also members of staff at Uplands, and respect their need for professional boundaries.

ALL IMAGES AND DATA STORED WILL COMPLY WITH DPA 2018 AND GDPR GUIDANCE

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

3.10.1 The internet has emerging online spaces and social networks which offer great potential for education. Collaboration tools such as discussion forums and newsgroups are exciting methods for pupils and teachers to share information and opinions. Blogs may provide commentary or news on a particular subject and can be used as a class diary to chronicle learning activities. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control. Unfortunately, many of these online spaces and tools allow individuals to publish unmediated content and therefore carry an e-safety risk of cyber-bullying and inappropriate contact.

3.10.2 To protect against this risk, the following statements will be applied:

- 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 should be taught how to address these issues
- Advice regarding the use of forums, social networking sites and messaging facilities will be provided for parents/carers through the school website and newsletter

3.10.3 As many children now have access to iPads and mobile phones 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, Uplands Primary School and 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 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.

PLEASE REFER TO THE BEHAVIOUR POLICY AND ANTI BULLYING POLICY FOR GUIDANCE ON CYBER BULLYING AND DEALING WITH ISSUES THAT OCCUR OUTSIDE OF THE SCHOOL PREMISES.

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

3.11.1 As educators, teaching staff, non-teaching staff and governors have a professional image to uphold, and how they conduct themselves online helps determine this image. The use of social networking sites, such as Facebook, Twitter, Snapchat and Instagram, is not forbidden, but staff are advised to treat with caution if used. The following recommendations are suggested to support safe use:

- 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 10 characters made up from a mixture of letters, numbers and other characters) and change it regularly
- Consider carefully the posts you make, 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.

3.11.2 In Uplands Primary School and Nursery, several staff members are also 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 not accepting friend requests from children, even if they are family friends:
  - Are the children of a legal age to be on that social media site?
  - Which parts, if any, 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 networking sites
- Be aware of local groups and sites and what they post on these open forums
- 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.

3.12 Risk management: mobile phones in school

3.12.1 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:

3.12.2 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 in the child's locker during school hours.

- Pupils in Year 6 only may bring a mobile phone to school. The phone must be turned off or placed on 'silent mode' and kept in the child's locker. The school governors and staff recognise that many Year 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.

3.12.3 For staff:

- Mobile phones should not be visible or used at all during lessons or times when children are present.
- On trips and activities, staff are required to communicate via school mobile phones where at all possible. With school mobile phones, staff may take pictures and send them to staff via official channels (e.g. school email accounts or Uplands OneDrive).
- 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 personal mobile phones to take digital media of any pupils, at any time. Staff may, however, use iPads, school cameras/video cameras or a school mobile phone.
- Smartwatches may not be used during lessons or when children are present. Notifications should be muted/set to Do Not Disturb on smartwatches, and should not be used for any form of communication.

3.12.4 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 read the visitors' cue card, which provides information on e-safety expectations.

3.13 Risk management: mobile phone use on residential and offsite 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/carers 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/carers are accompanying children and staff, they will be made aware of the expectations with regard to the above points.

4 Education in e-safety

4.1 Whilst managing information systems forms is 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.

4.2 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 EYFS 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 be shown how to validate information before accepting its accuracy
- Pupils will be taught to avoid hardware becoming infected with and transmitting computer viruses
- 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 near all relevant technology (Appendix C).

4.3 **Respecting Copyright**

Pupils 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

5.1 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, security breaches and access to inappropriate materials.

5.2 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 e-safety officers using the E-safety Incident Log (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)
- Access to the reported sites can be immediately blocked by the e-safety officers using RM Safety Net+ software
- Filtering is regularly checked by network manager, Internet Service Provider (ISP) and South East Grid for Learning (SEGfL). ISP monitors 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.

5.3 **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.

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

- All e-safety incidents are promptly reported to the named e-safety officers. The incident will then be recorded in the E-safety Incident Log (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 DSLs
- All incidents of misuse (from staff or pupils) will be promptly reported to the Head Teacher or e-safety officer
- 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 in the school community

6.1 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.

6.2 Involvement of staff

- Staff will have access to the E-Safety Policy and will sign an Acceptable Usage Policy to agree with its rules, restrictions and guidelines
- All new staff will be asked to read the E-Safety Policy on joining the school
- All 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 IT systems in school
    - Report any known misuse of technology and e-safety incidents as part of safeguarding training (e.g. the viewing of inappropriate material or cyber-bullying) to the e-safety officer or IT Technician. This information will then be passed on through the appropriate channels (see Appendix E)
    - Report any failings in network filters (e.g. inappropriate material being accessed) to the IT Technician using the E-Safety Incident Log (e-safety policy, Appendix D) and reported to the e-safety officer
- Staff understand that, in order to safeguard children, the following statements apply:
    - Uplands Primary School and 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 Uplands Primary School and Nursery and staff agree that their internet activity must be in keeping with their professional role or the children's education
    - Deliberate misuse of the network, electronic devices and IT systems may result in disciplinary action.

6.3 Involvement of pupils

- All pupils are made aware of their rights and responsibilities when using IT systems through the Pupils' Acceptable Usage Policy and posters (see Appendix C)
- The Pupils' Acceptable Usage Policy is posted in all rooms where computers are used, including classrooms, 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
- A module giving direct e-safety teaching and instruction is included in the 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

6.4 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 consent statements sent to parents/carers (Appendix B) details what parents/carers must give their consent to
- 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
- Advice on responsible use of the internet will be offered to parents through the school website.

6.5 Involvement of community

Internet access is available in many situations in the local community, including after-school child care facilities and clubs/organisations. 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

*** 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.**

Acceptable Usage Policy for the internet, electronic devices and general e-conduct (Staff)

This covers the use of electronic equipment, devices (hardware), software, apps and programs (e.g. email), as well as conduct related to e-safety and safeguarding children. By signing this form, you agree that you have read the e-safety policy in full and will follow all areas.

Failure to behave in accordance with the terms of this agreement may result in disciplinary action.

Staff member’s name	
Signature	
Date	

This is also linked to the Software/Hardware agreement.

Consent statements for parents/carers

I give consent for Uplands to take photos of my child for learning purposes.
These images are stored on a secure, encrypted server and cloud storage area and are also shared with some approved Data Processors for learning purposes. Any Data Processor Uplands uses is GDPR / DPA2018 compliant.
(Y/N)

I give consent for Uplands to take photos of my child for use in our:

- **Newsletter**
- **Website**
- **Social media posts (Facebook and Twitter)**
- **Displays and marketing materials (e.g. prospectus)**
- **Local and national news publications**

We request this in one group as it is not possible to guarantee one aspect but not others. For example, our newsletter is shared on the website and social media, so agreeing to the newsletter but not the website would cause unmanageable issues in adhering to your request. This also includes publishing in local newspapers such as Bracknell News, or larger newspapers. At events (such as sports tournaments), photographers attend to take photos for newspapers, and ask permission. By having permission already obtained (or not given), we are able to act on your behalf efficiently. Any Data Processor Uplands uses (such as a website provider) is GDPR / DPA2018 compliant. Social media platforms have their own privacy policies and processes.
(Y/N)

I give consent for my child to use the internet and electronic devices in school.
This is to ensure that children are able to access research and learn on a range of devices. All children receive e-safety training and are supported to use the devices.
(Y/N)

I give consent for my child to view media at Uplands, such as excerpts from films or documentaries, for learning purposes.
Age guidelines will be taken into account and the media checked for its appropriateness. All clips, regardless of age rating, will be checked by staff and deemed suitable for the class.
(Y/N)

EYFS and KS1 Acceptable Usage Policy for home and school

😊	**I will** only use a computer or tablet if there is an adult with me.
	I will tell an adult if I see anything I don’t like or am confused by.
	I will only send friendly and polite messages to people I know.
😔	**I will not** touch a computer or tablet if my hands are dirty or wet.
	I will not click on things an adult hasn’t shown me how to use.
	I will not turn the computer on or off unless an adult has agreed.
😃	**I understand** that these rules will help to keep me and my family safe.
	I understand these rules.

Key Stage 2 Acceptable Usage Policy for home and school

I will ask permission before using the internet.
I will only open and delete my own files.
I will only email and open email attachments from people I know, or who my teacher has approved.
I will make sure that all ICT contact with other children and adults is polite and sensible.
I will tell my teacher right away if I come across any information which I don’t like or makes me feel uncomfortable.
I will not give out personal information like my name, address, telephone number, picture or the name and location of my school without permission.
I will not agree to get together with someone I “meet” online.
I will not give out my ICT passwords to anyone other than my teacher (not even to my best friends).
I will not download or install any software.
I will not use USB drives or other external devices from outside school unless my teacher says I can.
I will not deliberately look for, save or send anything that could be unpleasant or nasty.
I will not reply to messages that are mean or make me feel uncomfortable. Instead I will tell my teacher right away.
I will not upload or post any pictures of other children on to the internet including social networking sites.
I understand that my teachers can check what I am doing to make sure I am behaving responsibly and staying safe.

E-safety Incident Log

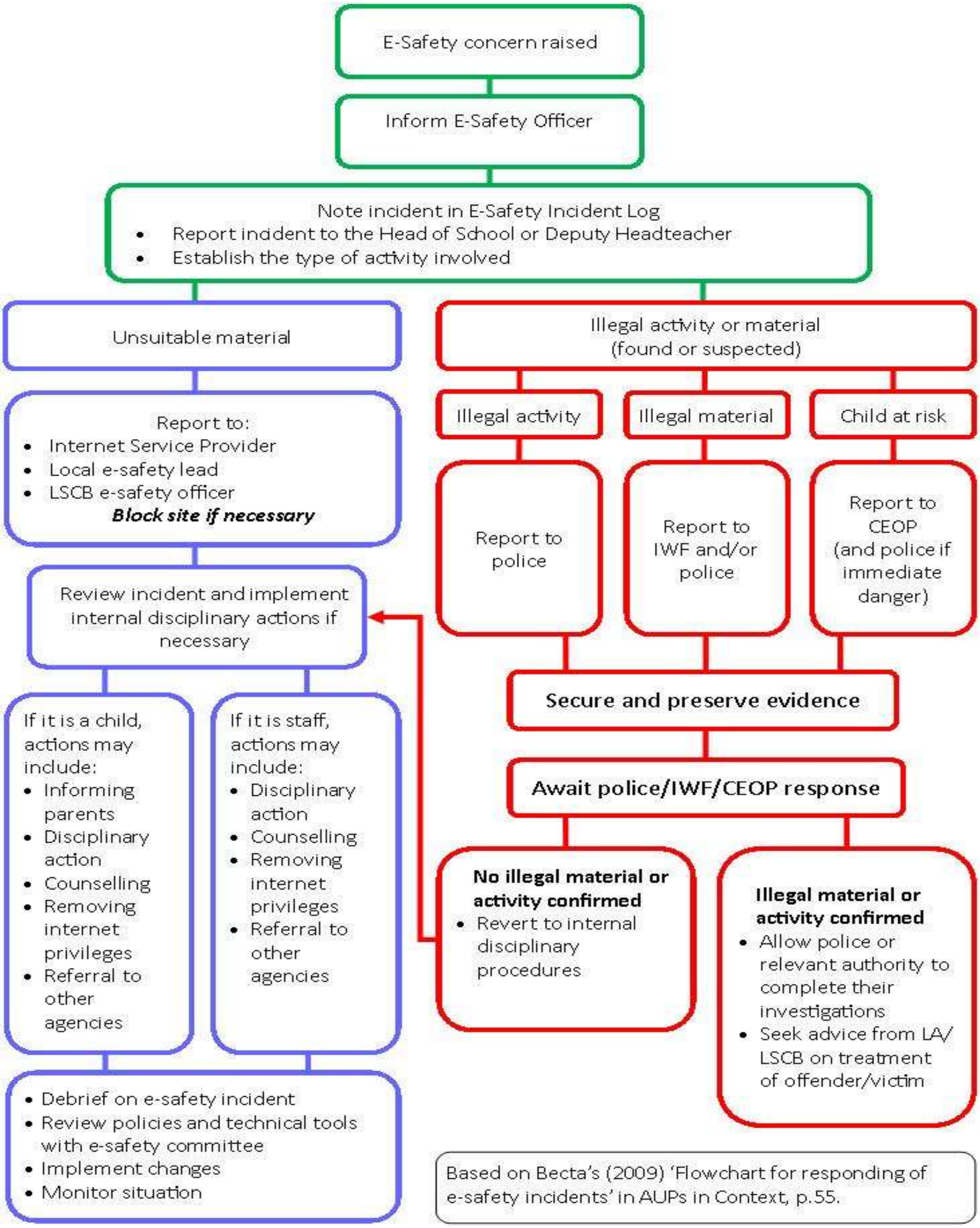
Details of **ALL** e-safety incidents are to be reported to and recorded by the named e-safety officer.

All incidents will be escalated according to the E-safety Incident Response Flowchart (see Appendix E) in line with Becta advice.

The incident log will be monitored termly by the Head Teacher and the e-safety committee.

Date & Time	Name of pupil or staff member	Male or Female	Room & device number	Details of incident (including evidence)	Actions and Reasons

E-safety Incident Escalation Flowchart


E-Safety concern raised
Inform E-Safety Officer
Note incident in E-Safety Incident Log
• Report incident to the Head of School or Deputy Headteacher
• Establish the type of activity involved
Unsuitable material
Illegal activity or material (found or suspected)
Illegal activity
Illegal material
Child at risk
Report to: • Internet Service Provider • Local e-safety lead • LSCB e-safety officer
Block site if necessary
Report to police
Report to IWF and/or police
Report to CEOP (and police if immediate danger)
Review incident and implement internal disciplinary actions if necessary
Secure and preserve evidence
Await police/IWF/CEOP response
If it is a child, actions may include: • Informing parents • Disciplinary action • Counselling • Removing internet privileges • Referral to other agencies
If it is staff, actions may include: • Disciplinary action • Counselling • Removing internet privileges • Referral to other agencies
No illegal material or activity confirmed • Revert to internal disciplinary procedures
Illegal material or activity confirmed • Allow police or relevant authority to complete their investigations • Seek advice from LA/ LSCB on treatment of offender/victim
• Debrief on e-safety incident • Review policies and technical tools with e-safety committee • Implement changes • Monitor situation

Based on Becta's (2009) 'Flowchart for responding of e-safety incidents' in AUPs in Context, p.55.

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

Managing incidents support form
The e-safety officer/DSL 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 officer/DSL
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 officer/DSL
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 officer/DSL
2. Secure and preserve any evidence
3. In the case of offending web-based emails 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 officer/DSL
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

Password guidance

Passwords ensure that our data is safe and personal details are secure. This is essential in an organisation such as ours, where we have child and staff data within our system. The following guidelines should be applied to all passwords created within the Uplands systems and programs.

Use passwords of at least 8 characters
The more characters, the more difficult a password is to crack. Length is key. There are 6,630,000,000,000,000 (in American terms, 6.63 quadrillion) combinations of passwords with 8 characters and letters, so you've got a few options!

Create a unique password
Each password you use should be for a unique service (Microsoft 365, ASP etc. should all have a different password).

Use a combination of character types
Use numbers, lowercase letters, uppercase letters and symbols in your password wherever you can. A small number of sites won't let you use symbols, but most will allow characters such as "@" and "!" (e.g. e*Xp10d@b!3).*

Change your password regularly
It is recommended that you change your personal passwords **at least** every six months, if not every three months. This is best practice.

Consider using a randomly generated password
Use one of the following sites to generate a secure password:

- Norton by Symantec
- Random.org
- Random Password Generator

Create a password you remember, but others can't see easily!
A password like **@7X#JjI6j4e#cC2axjFz%j@* is likely going to be difficult for most people to remember. But, a long password is difficult to crack, and can be crafted from some common piece of information.

Using the first letter of each word in a quote from a film or favourite line from a song is always a good way to create a password that you will remember, but that isn't obvious to others, e.g. "Under the Boardwalk" could become "UtB0@rdw4!k"

DO NOT use password managers
Password Managers can remember passwords for users. We do not recommend the use of Password Managers as they are a gateway to **all** of your passwords. Having one password that can access all the rest of your passwords and sites is certainly very risky, and against best practice.

DO NOT use dictionary words
This one should be obvious. If your password is *documentation*, your data is probably already hacked.

DO NOT use pets, people, places, events etc. (unless a range of characters used)
We're absolutely sure your dog is adorable, but her name probably isn't a good password. Unless her name is *Tmb1W\>r~ii*, in which case that's acceptable.

DO NOT reuse passwords
Let's say your first password for an account was *gCB7%TT^Vm* but you were forced to change your password, so you changed it to *v8@#TsVaiQ*. If you have to change the password for that account again, do NOT go back to *gCB7%TT^Vm*. Create a new, unique password instead.

DO NOT use adjacent keyboard strings
qwerty1234 is not a good password.

Password examples

Weak (bad)	Strong (good)
awesomedog	C@tastr0ph333
sunshine12	0nC3Up0N4T!m3
coolguy18	D0n!tC4m3@rg3nt!n4
kerri28	
password	