Uplands Manor Primary School

E-safety Policy

Date approved by Governors: 11th July 2016

Mr D Feiven
Chair of Governors

Mr P Moore
Headteacher

Purpose of our e-Safety Policy

Rationale

As the use of online services and resources grows, so has awareness of the risks and potential dangers which arise from the use of communications technology and the internet. Those risks are not confined to the use of computers; they may also arise through the use of other handheld devices such as games consoles and mobile phones.

Children interact with new technologies on a daily basis. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally, if not used correctly, place children and young people in danger.

Our e-Safety Policy covers issues relating to children and young people and their safe use of the Internet, mobile phones, handheld devices and other electronic communications technologies, both in and out of school. It includes educating children on the risks and responsibilities of using such technologies safely and is part of the "duty of care" which applies to everyone working with children. Uplands Manor Primary School will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

E-Safety at Uplands Manor Primary School is embedded in effective practice in each of the following areas:

- Education for responsible ICT use by all staff and pupils;
- A comprehensive, agreed and implemented e-Safety Policy;
- Use of a secure, filtered broadband (Broadband Sandwell);
- A school network that complies with the National Education Network standards and specifications.

The policy is one of the strategies Uplands Manor Primary School has in place to promote the safety of learners in their care both when they are in the school and when they are elsewhere.

Communications of this Policy

This e-Safety Policy has been written by the school, building on Local Authority and government guidance and through period of consultation with staff. It will be approved by Governors and the School Leadership Team. This policy will be available on the school's website and on Openhive, and has been read by all staff.

Parents will be made aware that the school has a policy on e-safety and will be advised on ways of keeping their children safe at home
It is the responsibility of all staff to ensure that they use communications technology and the internet safely and responsibly. To this end, all staff agree to an acceptable use policy (AUP).

Introducing the e-Safety Policy to pupils:

- e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up
- E-Safety will be taught based on the materials from the Child Exploitation and Online Protection Centre (CEOP.)
- E-Safety training will be embedded within the whole school curriculum.
- All children and young people require safe opportunities to understand the risks and benefits of the Internet and to balance these in their everyday use

Staff and the e-Safety policy:

- All staff will be given the School's e-Safety policy and emphasise its importance
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user
- Where appropriate, staff will always try use a child friendly, safe search engine when accessing the web with pupils e.g. "Yahoo Kids"
- Regular e-Safety training will be part of the school's continuing Professional Development (CPD) programme

Parents and the e-Safety Policy:

- Parents' and carers' attention will be drawn to the school's e-Safety policy in newsletters, the school brochure and on the school's web site
- The school will maintain a list of e-Safety resources for parents/carers which will be attached to the e-safety policy and available on the school website
- e-Safety support, guidance, advice and/or workshops will be offered to parents/carers with an e-Safety support contact available on the school's website

1. Internet Use in School

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

The use of the internet and digital communications is a part of the statutory curriculum and a necessary tool for staff and pupils.

The purpose of Internet use at Uplands Manor Primary School is to:

- Raise educational standards
- Promote achievements
- Support the professional work of staff
- Enhance management systems
- Provide information to parents and the wider community

Children also use the Internet regularly outside school to support their learning as well as for recreational reasons. The quality of the information received via the internet is variable. It is really important, therefore, for children to be taught the appropriate skills to select and evaluate internet content. It is also important that children know that they should report any unsuitable material to an adult immediately.

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

E-Safety Actions

In the curriculum at Uplands Manor Primary School, pupils will:

- Be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Be educated in the effective use of the Internet to research, including the skills of retrieval and evaluation.
- Be shown how to publish and present information to a wider audience.
- Be taught how to evaluate the relevance, accuracy and quality of Internet sourced material
- Be taught the importance of cross-checking information before accepting its accuracy
- Be supervised when using the Internet
- Be taught how to report unpleasant Internet content by using the Child Exploitation and Online Protection Centre (CEOP) “Report Abuse” icon or similar systems.
- Know what to do if they experience any issues whilst online

***The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use*.**

2. Managing Internet Access

a. Information system security

It is important that a school reviews and maintains the security of the whole computer and ICT system. This ensures the on-going delivery of essential learning services as well as the personal safety of staff and pupils. Maintaining computer security is a major responsibility of a school. It is a complex matter and will not be covered in full in this document.

E-Safety Actions

- The security of the school's information systems is reviewed regularly by the Network Manager, Computing Leader, Head Teacher
- Virus protection is updated regularly
- Use of the Froglearn and OPENHIVE ensures that all data sent by email is secure and all data stored on the platform is secure.
- Files held on the school's network are regularly checked and modified or deleted when necessary
- Managing filtering:
- The school will work with the Sandwell Local Authority and a managed filtering system (Broadband Sandwell) to ensure systems in place to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator or the Head Teacher.
- Children are taught to turn off the monitor immediately when any unsuitable material appears, and notify an appropriate adult.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

b. Email

Email is an essential means of communication for staff, staff will also communicate and share information on Openhive. Pupils however will not have school emails as E-mails as they can be difficult to monitor and unregulated e-mail can leave pupils exposed to influences outside what is acceptable in school. Children will be able to communicate on Frog.

E-Safety Actions

- Children only use their Froglearn accounts to communicate
- Pupils will be given a username and password to use the schools Learning Platform – Froglearn.
- Children tell an adult immediately if they receive an offensive message
- Staff emails are monitored for profanity and reported if this takes place.
- Open hive is regularly monitored and any abuse is reported to the SLT.

c. Published content and the school web site

Uplands Manor Primary School will regularly publish information. Personal information should only be held on secure systems which are accessed by authorised staff whereas general information about the school may be published wider. Froglearn is an effective way of publishing information relevant to the school, families and community as it requires authentication while reaching a wide and relevant audience however, sometimes it is useful to use the website. In these cases consideration of personal and school security is essential.

E-Safety Actions

- The contact details on the website and the office e-mail and telephone number. Staff or children's information is not shared.
- The Head Teacher has overall editorial responsibility for the website to ensure that content is accurate and appropriate
- Parents or carers give written permission for images of children and their work to be posted on the website.

3. Social networking and personal publishing:

Parents and teachers need to be aware that the Internet has online spaces and social networking sites which allow children to publish content (e.g., photos, comments and personal information). These sites should only be viewed by invited 'friends'. All staff should amend settings to ensure their status and photos cannot be shared by anyone, by using networking sites permissions settings.

When used by responsible adults social networking sites provide easy to use free facilities however children should be encouraged to think about the issues related to uploading personal information before signing up to social networking. Children are discouraged to sign up to online spaces or social networking sites due to age restrictions.

We have a school Facebook and twitter account which we monitor closely to ensure staff, parents and pupils use it appropriately.

E-Safety Actions

- The school blocks access to general social networking sites
- Children are taught about the dangers (including bullying) of sharing personal information, especially on-line
- Staff who use social networking sites must be aware of the nature of what they are publishing on-line in relation to their professional position
- If staff are signed up to social networking sites they must not discuss any matters relating to the school, children or their professional role on-line.
- Staff do not invite children to be 'friends' on-line and equally do not accept requests for friendship from children or passed pupils of the school
- Where necessary, the school will closely control access to and the use of school accepted social networking sites, with consideration given as to how the pupils can be educated in their safe usage.
- Pupils and staff will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils will be taught not to meet anyone first met online without specific permission or a responsible adult present.
- Pupils are encouraged to only ever use moderated social networking sites.
- Pupils and parents will be strongly advised of age restrictions of social networking sites that the use of social network spaces outside school may bring a range of dangers to all pupils.

a. Managing emerging technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tool, including mobile communications and multimedia. A risk assessment needs to be undertaken on each new technology before using it with children. The safest approach is to deny access until a risk assessment has been completed and safety demonstrated.

E-Safety Actions

- Emerging technologies are examined for educational benefit and a risk assessment will be carried out before use in school is permitted
- If mobile phones are brought into school by children for safety purposes getting to and from school, they are placed in the school safe then returned at the end of the school day
- Personal mobiles and personal digital cameras should not normally be used to record sound and images during the school day
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new access route to undesirable material and communications.

- When mobile technology is used in the classroom, clear ground rules must be established for its safe and appropriate use.
- School digital cameras are not to be taken off the school site (with the exception of school trips).
- Any photographs or videos taken on any handheld devices are to be used in school for educational purposes only, or to create a record of children's activities for use in class or to be uploaded onto the website. Once photographs or videos are downloaded from a handheld device, they will be deleted from that device. In particular, any handheld devices which are taken off school premises, must be cleared of school photos before being removed.
- The appropriate use of Learning Platforms will be reviewed as the technology becomes available within the school.
- Pupils will be given a username and password to access Froglearn, the school's Learning Platform.
- The educational benefits of mobile technology will be encouraged but not misused.

4. Leadership in e-Safety

The Deputy Headteacher for Behaviour and Safety is the e-safety co-ordinator.

a. Data Protection

The quality and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is handled properly. The Head Teacher is responsible for ensuring the Data Protection procedures are in place.

E-Safety Actions

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998
- Staff will not store data related to children, families or school on a removable storage device.

b. Complaints Procedure

Keeping in line with school policy, if a member of staff, child, parent or carer has a complaint relating to e-safety then it will be considered and prompt action will be taken following an immediate investigation.

E-Safety Actions

- Parents will be provided with advice on the Frog Portal and through e-safety meetings or workshops
- Parents will be made aware of the schools e-safety policy and the AUP agreements signed by children
- The school liaises with local schools and organisations to establish a common approach to e-safety
- The school will offer parents and families advice on matters of e- safety e.g., social networking sites and monitoring child access at home
- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. (Appendix 1 displays a flowchart of responses to an incident of concern.)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

c. Authorising Internet access

E-safety Actions

- All staff must read and sign the Staff Acceptable Use Policy for ICT before using any school ICT resource.
- At Uplands Manor Primary School, access to the Internet will be with adult supervision and will only access specific, approved on-line materials.

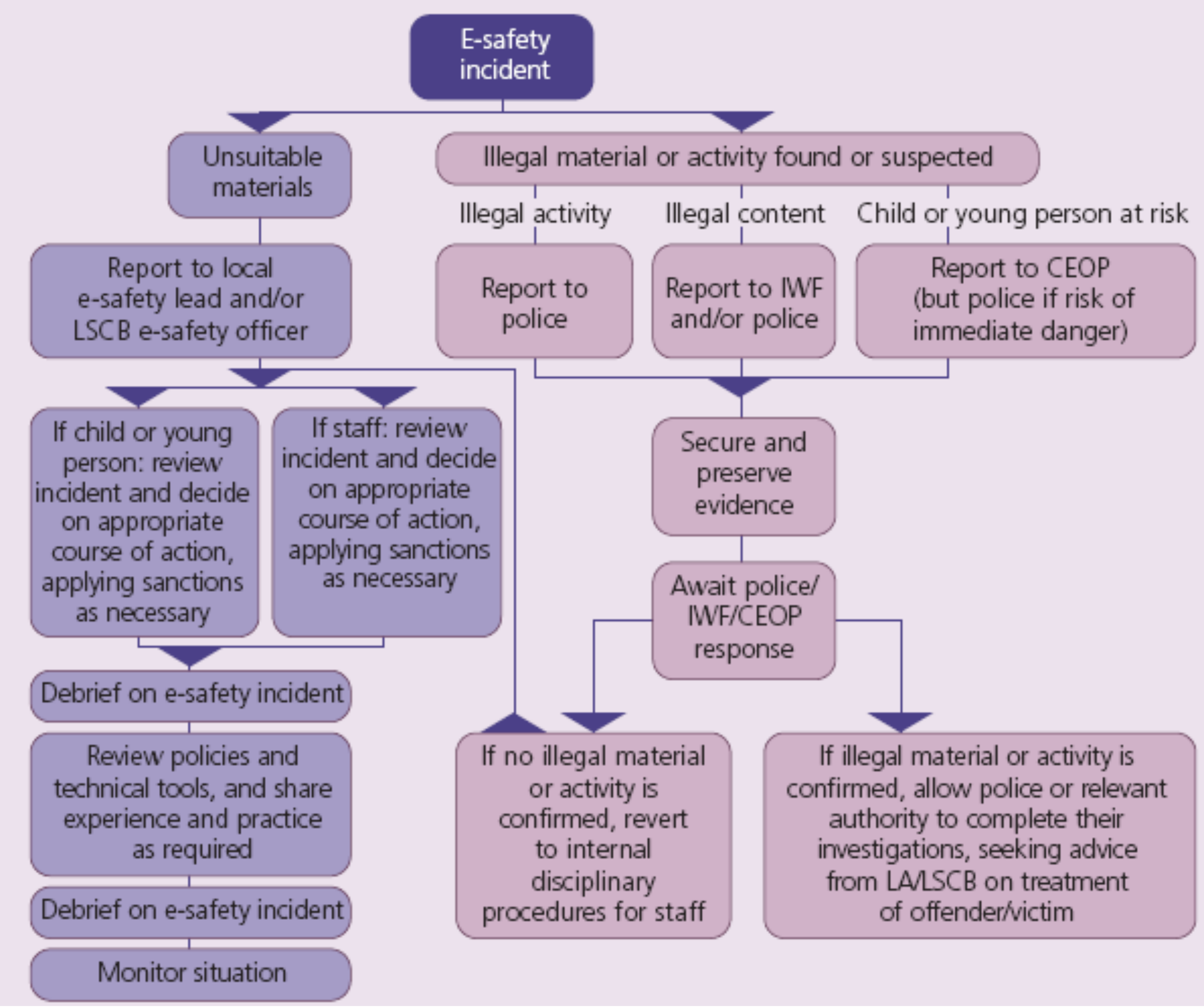
d. Assessing risks

e-safety Actions

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Sandwell Local Authority can accept liability for any material accessed or any consequences of Internet access.

- The school will carry out an annual audit of ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Appendix 1: Flowchart for responding to e-safety incidents


E-safety incident
Unsuitable materials
Illegal material or activity found or suspected
Illegal activity
Illegal content
Child or young person at risk
Report to local e-safety lead and/or LSCB e-safety officer
Report to police
Report to IWF and/or police
Report to CEOP (but police if risk of immediate danger)
If child or young person: review incident and decide on appropriate course of action, applying sanctions as necessary
If staff: review incident and decide on appropriate course of action, applying sanctions as necessary
Secure and preserve evidence
Await police/ IWF/CEOP response
Debrief on e-safety incident
Review policies and technical tools, and share experience and practice as required
Debrief on e-safety incident
Monitor situation
If no illegal material or activity is confirmed, revert to internal disciplinary procedures for staff
If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations, seeking advice from LA/LSCB on treatment of offender/victim

(Figure reproduced from Becta - *Safeguarding children online: a guide for Local Authorities and Local Safeguarding Children Boards*, page 27, appendix B)

Appendix 2 - Acceptable Use Policies

I agree that I will:

- Always log off a computer when leaving, even if it is only for a short while
- Only use personal data securely
- Educate children in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Educate children in the recognition of bias, unreliability and validity of sources
- Actively educate learners to respect copyright law
- Only use approved school OPENHIVE e-mail accounts in school and for school related emails
- Only use pupil images or work when approved by parents and in a way that will not enable individual children to be identified
- Only give access to appropriate users when working with blogs or wikis etc.
- Report unsuitable content or activities to the computing coordinator/computing technician
- Pass on any examples of Internet misuse to a senior member of staff
- Ensure that any personal use of ICT does not interfere with my professional duties or use physical resources

I agree that I will not:

- Share my password with others or work on a computer using someone else's password, unless they are overseeing the work
- Store data relating to the children, families or school on a removable storage device (e.g. data stick)
- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - pornography (including child pornography)
    - promoting discrimination of any kind
    - promoting racial or religious hatred
    - promoting illegal acts
    - breaching any Local Authority/School policies, e.g., gambling
    - doing anything which exposes children to danger
    - any other information which may be offensive to colleagues:
        - forward chain letters
        - breach copyright law
        - knowingly distribute a computer virus
        - install hardware or software without permission from the
        - Computing Coordinator, Computing technician or Head Teacher

I accept that my use of the school and Local Authority ICT facilities will be monitored and the outcomes of the monitoring may be used. I also accept that whatever I save to the Network maybe modified or deleted without my consent.

Signed: *Date:*

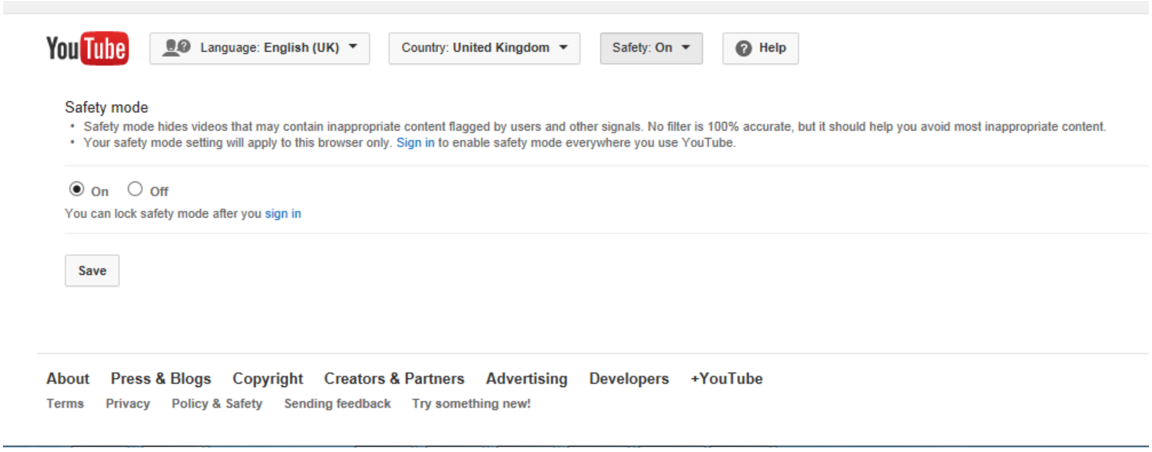
Acceptable Use - Uplands Manor Primary School YouTube Policy

It has been agreed by our Head Teacher and Governors to enable the use of YouTube for staff to support teaching and learning. This access comes with a high responsibility as often images and text can be seen on a YouTube screen that you would not want a child at Uplands to see.

It is important to remember that, whilst YouTube itself requests a community of trust, there may still be videos that we would not want children at Uplands to see. It must be noted that the minimum age for adding videos is 13 years old.

When staff use YouTube in school the following must be adhered to:

- You Tube videos are to be embedded into Frog to share with the children.
- All videos used must be pre-searched and a check carried out for inappropriate language and images before being used with children.
- Be aware of what is around the video – advertisements etc.
- All videos must be viewed before showing children.
- Don't leave yourself logged on if you have finished your session on the whiteboard. Your computer must be locked when you leave the room.
- Your password for the computer must be secure, it MUST NOT be shared with any children.
- Safe search needs to be on.



Language: English (UK) Country: United Kingdom Safety: On

Safety mode

- Safety mode hides videos that may contain inappropriate content flagged by users and other signals. No filter is 100% accurate, but it should help you avoid most inappropriate content.
- Your safety mode setting will apply to this browser only. Sign in to enable safety mode everywhere you use YouTube.

● On ○ Off

You can lock safety mode after you sign in

Google – educator's resource when using YouTube:
https://support.google.com/youtube/answer/2802327
Secondary view of using YouTube to support teaching and learning:
http://www.youtube.com/user/teachers

I have read and understood the YouTube policy for Uplands Manor Primary School.

Signed ……………………………………………………………………….

Print Name ……………………………………………………