Internet Safety Policy

Introduction:
Arbury primary school encourages the use of the Internet to promote learning in a wide range of areas. Exploiting the online world is now a key means of extending and personalising the educational experience of all learners.

School governors, including the headteacher, share with the head of local authority children's services personal responsibility for the safety of their school's children and young people. This responsibility extends to safe use of online facilities provided by the school.

Aims:
This policy focuses on the personal safety and well being of pupils at Arbury Primary School. It aims to clarify the potential risks and details the steps that staff can take to minimise those risks. It is principally concerned with safe use of the Internet and considers the content children are uploading as well as what they are downloading.

Learning to use the resources of the Internet safely and appropriately is an important part of the education of all pupils. Internet Safety is incorporated into the curriculum, mainly through the computing curriculum and PSHE schemes of work and weekly lessons.

Acceptable Use Policy:
Adults working in schools should observe our Acceptable Use Policy (AUP). (Appendix 1)
Children should follow the 'Responsible Internet Use' guidance which has been shared with parents and links more closely with their 'eSchools' accounts. (Appendix 2)

Bullying and Abuse:
The communication systems referred to in this policy can be misused to offend, upset or intimidate pupils or staff both in school and outside. This is sometimes described as cyberbullying. Such incidents will be dealt with through the school's Behaviour Policy.

Internet Service Providers:

Arbury Primary School uses a filtered internet feed recommended by the local authority ICT Service called 'EasyNet' which has web filtering and safeguarding alerts and reporting through 'Smoothwall'. Enterprise level security and web filtering solutions are included. It has been implemented to align with the latest guidance and along the principles of Keeping Children Safe in Education.

Smoothwall scans the copies, content and context of every page for unwanted material and has 120 filtering categories which can be used to tailor the web browsing experience and ensure that harmful content is out of reach. Alerts for attempted access are sent to the DSL/DDSL team so that this can be followed up either through an individual login on windows devices or an address of a shared device such as an iPad.

We understand that even the best filters cannot eliminate the risk of exposure to inappropriate material. We will ensure the suitable positioning of screens to ensure that staff can monitor what children are accessing. Children will not use the Internet unless a member of staff is present.

Search Engines:
We acknowledge that because of the huge scale of the Internet, we will use search engines to help find relevant material. An innocent search can result in offensive sites being listed, and even if the filtering system prevents the user from following a link to the site in question, sufficient information can be displayed in the search results to upset or offend.

The Smoothwall service will allow schools to use Google more confidently. It will enforce the 'Very Safe Search' option, and in Google image searches it will prevent the display of thumbnail images from blocked sites. Smoothwall will often stop the search from being run at all.

Publishing Information on the Internet
We acknowledge that pictures, names, addresses, ages or information about a child's likes or dislikes can be used to trace, contact and meet a pupil with the intention of causing harm.

On no account should either first names or surnames be attached to photos of children on websites. Care must be exercised that the filename of a photograph (e.g. janesmith.jpg) does not inadvertently identify a child.

Photographs of children, in which individuals can be identified, will only be used on the website if the school has written permission. Parents may withdraw permission at any time by contacting the school office.

Using E-mail:
Through their eSchools accounts, children can send and receive messages from children within the school only. All emails sent and received from pupil accounts can be monitored and pupils are aware that this is possible.

Members of staff who communicate with children by e-mail should only send messages from and to the official class accounts provided by their schools, since these can be audited if there are any suggestions of misuse. Class accounts can also be used by members of staff to send and receive emails outside of the school community.

Pupils should inform their teacher if they receive abusive or unwanted messages of any kind. A senior member of staff will investigate and this could lead to a child's account being suspended.

Chatrooms:
Chatrooms enable users to engage in real time 'conversations' with people across the street or across the world. They are similar to telephone conversations except that messages are typed instead of spoken. Usually everyone in a chatroom can see all the other participants' contributions. Unlike email, once chat sessions are finished there will often be no obvious record of what has been posted.

Our curriculum will highlight the danger to children of public chatroom use where people do not necessarily tell the truth about who they are. Children will be taught not to provide personal information, as it is possible that they could be traced and contacted by another user who could then cause harm.

Chatroom use in school will be restricted to using eSchools which allows teachers to set up secure chat sessions where they can control who is taking part and when they occur.

Online games:
Multi-player online games also provide opportunities for players to communicate with each other, often using an invented identity. They can be absorbing and exciting and can develop problem solving skills and collaborative learning. In these situations, the same precautions need to be taken as in chat rooms.

Social Networking:
Social Networking areas are websites, which help connect friends using a number of tools like blogs, profiles, internal email systems and photos. They can be customised, and pictures, video and music can be uploaded and shared. They can bring users into contact with strangers by developing networks of "friends of friends".

While children will not be using these sites in school, they are increasingly likely to form part of their out-of-school life, and e-safety programmes should take account of this. We will Monitor the age limits of popular apps and will advise children and families as needed.

Online Learning Platforms:
We will be providing the opportunity for pupils to use an online learning platform, which has controlled access. This online learning platform offers many easy-to-use communication and collaboration tools enabling online communities to be created with the restricted membership of pupils in the school.

The online learning platform offers a measure of security by limiting access to authorised members. A number of facilities such as web publishing, e-mail, online discussion and chat are available, with an increased level of safety compared to completely open use of the Internet. Teachers and pupils still need to adopt a careful approach. Pupils should inform their teacher if they receive unwanted messages. Membership of the online community is restricted to pupils attending the school.

The school's 'Responsible Internet Use' guidance for pupils details our expectations for children using the internet and their online learning platform. (Appendix 2)

Prevention of Online Radicalisation

Since 2010, when the Government published the Prevent Strategy, there has been an awareness of the specific need to safeguard children, young people and families from violent extremism. There have been several occasions both locally and nationally in which extremist groups have attempted to radicalise vulnerable children and young people to hold extreme views including views justifying political, religious, sexist or racist violence, or to steer them into a rigid and narrow ideology that is intolerant of diversity and leaves them vulnerable to future radicalisation.

The current threat from terrorism in the United Kingdom may include the exploitation of vulnerable people, to involve them in terrorism or in activity in support of terrorism. The normalisation of extreme views may also make children and young people vulnerable to future manipulation and exploitation. Arbury Primary School is clear that this exploitation and radicalisation should be viewed as a safeguarding concern.

The Counter-terrorism and Security Act, 2015 places a duty on authorities (including schools) 'to have due regard to the need to prevent people from being drawn into terrorism'. Staff in schools have been made aware of this duty. When any member of staff has concerns that a pupil may be at risk of radicalisation or involvement in terrorism, they will speak with the Designated Safeguarding Lead who may pass on information to the local authority.

Written – 2008
Reviewed – June 2010 by Headteacher
Adopted by Full Governing Body – June 2010
Amended by Full Governors – October 2011
Amended by Curriculum Committee – June 2013
Amended – Sept 2015 in light of 'Prevent' training
Amended – May 2017
Reviewed – July 2019 by BT/SE
Reviewed / Amended – May 2023 - BT

Appendix 1

Acceptable Use Policy – Staff Guidance

- All members of staff are issued with their own unique user id and password to ensure there is accountability and an audit trail of their activities. Staff should to never divulge their passwords to anyone.

- Staff should not leave themselves logged on when they leave a computer unattended. Computers should be configured to present a screen lock and authentication challenge after a period of inactivity. This is to protect against unauthorised access.

- Staff should change their passwords regularly. The network should be set up to ask for a password change every month.

- Staff using the Internet are expected not to deliberately seek out offensive materials. Staff who believe that an inappropriate item has passed through the filter should report it to the DSL/DDSL.

- Staff Members who communicate with children by e-mail should only send messages from and to the official class accounts provided by their schools, since these can be audited if there are any suggestions of misuse.

- Photographs of children, in which individuals can be identified, will only be used on the website if the school has written permission. Parents may withdraw permission at any time by contacting the school office

- Staff should not install software to the computer from the Internet or other media unless with the permission of the headteacher or computing co-ordinator.

- Staff should understand that this guidance also applies to the off-site use of school equipment and portable equipment brought into school.

Action to be taken if misuse is suspected:

- The local authority ICT Service will be able to assist the school if there are concerns about access to child sex abuse images or any other illegal material.

- The device will be immediately powered down and removed from service, the local authority will be contacted immediately and arrangements will be made for the device to be examined.

Prevention of Online Radicalisation

Since 2010, when the Government published the Prevent Strategy, there has been an awareness of the specific need to safeguard children, young people and families from violent extremism. There have been several occasions both locally and nationally in which extremist groups have attempted to radicalise vulnerable children and young people to hold extreme views including views justifying political, religious, sexist or racist violence, or to steer them into a rigid and narrow ideology that is intolerant of diversity and leaves them vulnerable to future radicalisation.

The current threat from terrorism in the United Kingdom may include the exploitation of vulnerable people, to involve them in terrorism or in activity in support of terrorism. The normalisation of extreme views may also make children and young people vulnerable to future manipulation and exploitation. Arbury Primary School is clear that this exploitation and radicalisation should be viewed as a safeguarding concern.

The Counter-terrorism and Security Act, 2015 places a duty on authorities (including schools) 'to have due regard to the need to prevent people from being drawn into terrorism'. Staff in schools have been made aware of this duty. When any member of staff has concerns that a member of the school community may be at risk of radicalisation or involvement in terrorism, they will speak with the Designated Safeguarding Lead who may pass on information to the local authority.

I have read the 'Internet Safety Policy' and the 'Acceptable Use Policy – Staff Guidance' and agree to these safety restrictions:

Signed _____

Print _____

Arbury Primary School

Pupil Responsible Internet Use

- I will only use the computers / tablets for school work and homework
- I will only use the Internet when there is a teacher with me
- I understand that the school may check my computer files and messages I have sent and received, and may monitor the Internet sites I visit
- I will not access files belonging to other people unless I have permission to do so from my teacher
- I understand that when I communicate with people using the Internet, I must not give them my home address or phone number, or arrange to meet them without supervision
- I will tell a teacher immediately if I see anything I am unhappy with or I receive messages I do not like
- I will only use my own eSchools login and password, which I will keep secret
- Messages I send via eSchools, from school or home, will be polite and sensible
- I understand that my account may be stopped and my parents/carers will be informed if I do not follow these rules.