Online Safety Policy

School	Heytesbury C of E Primary School
Author	Emma Stevens
Last Amended	June 2021
Review Date	June 2022

Our online policy has been written by the school, building on the Wiltshire online template policy and government guidance. The policy should be read and used in conjunction with other school policies and documents, such as the behaviour, anti-bullying, personal, safeguarding and Staff Code of Conduct for Safer Working Practice.

Internet access for pupils should be seen as an entitlement on the basis of educational need and an essential resource for staff. Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Levels of access and supervision will vary according to the pupil's age and experience. Internet access must be appropriate for all members of the school community from the youngest pupil to staff.

- The school will work in partnership with parents, DFE and its ISP to ensure systems to protect pupils are reviewed and improved.
- Any material that the school believes is illegal or may place an individual at risk must be referred to the Head teacher and computing lead.

Risk Assessment

As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system.

- 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 access only appropriate 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 school computer. Heytesbury School and/or Acorn Trust cannot accept liability for the material accessed, or any consequences of Internet access.
- The computing subject lead will ensure that the Internet policy is implemented.
- The policy will be reviewed annually.

Teaching and Learning

The Curriculum

- Whilst Internet access is an entitlement, users will need to show a responsible and mature approach to its use or this privilege may be removed.
- The Internet is an essential part of everyday 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.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- Pupils will be taught to be critically aware of the materials they read and how to validate information before accepting its accuracy.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law and intellectual property.
- All pupils must receive E-safety education regularly throughout the school year.

Remote learning

While remote learning, all work will be set through the use of the school website. Children have been taught how to log on safely and navigate there way around their class dashboards. Parents/ carers must provide permission for children to take part in online lessons prior to remote learning taking place.

All staff and pupils using audio and or video communication must:

• Communicate in groups – one-to-one sessions are only carried out where necessary.
• Wear suitable clothing – this includes others in their household.
• Use appropriate language – this includes others in their household.
• Maintain the standard of behaviour expected in school.
• Use the necessary equipment and computer programs as intended.
• Not record, store, or distribute video material without permission.

The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for pupils with SEND. This will be decided and approved by the SLT, in collaboration with the SENCO.
Pupils not using devices or software as intended will be disciplined in line with the Behaviour Policy.
The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During the period of remote learning, the school will maintain regular contact with parents to:
• Reinforce the importance of children staying safe online.
• Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
• Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
• Direct parents to useful resources to help them keep their children safe online.

Communication and Content

Website Content

- The point of contact on the school website should be the school address, school e-mail and telephone number. Staff or pupils' personal information must not be published.
- Written permission from individuals, parents or carers will be obtained before photographs of pupils are published on the school website. Pupils' full names will not be used anywhere on the website.
- The nature of all items uploaded will not include content that allows the pupils to be identified, either individually or through aggregated pieces of information.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- Staff **must** use official school provided email accounts for all professional communications.

On-line communications and Social Media.

Pupils should be taught to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

Staff will not communicate through social networking sites with pupils or parents.

- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- No member of the school community i.e parents, carers, volunteers, staff and govenors, should publish specific and detailed private thoughts about the school, especially those that may be considered threatening, hurtful or defamatory.
- Parents may wish to take photos at school events of their child, but must never publish photos that include other children on social media.
- Concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning pupils' underage use of sites.

- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school's code of conduct.

Mobile Devices

Mobile devices refer to any device that provides access to the internet or internal network for example, tablet (Apple Android, Windows, and other operating systems) e-readers, mobile phone, iPad, iPod touch, digital cameras.

- During school hours staff **must** ensure that their mobile phone is in their bag, unless there is an exceptional circumstance, in which case the individual must seek permission from the head teacher.
- The school accepts no responsibility for the loss, theft or damage of such items.
- School staff authorised by the Head teacher may confiscate any mobile device they believe is being used to contravene school policy, constitute a prohibited item, is considered harmful, or detrimental to school discipline. If it is suspected that the material contained on the mobile device relates to a criminal offence, the device will be handed over to the Police for investigation.
- Where staff may need to contact children, young people and their families within or outside of the setting in a professional capacity, they should only do so via an approved school account (e.g. e-mail, phone, social media) In exceptional circumstances there may be a need to use their own personal devices and account; this should be notified to a senior member of staff ASAP.
- Staff should be provided with school equipment for the taking photos or videos of pupils linked to an educational intention. Photo must not be taken on a mobile phone.
- Pupils must not have mobile phones in school expect in exceptional circumstances where therefore in this situation, phones must be locked in the office. The school will not take responsibility for the device.

Cyber Bullying

Cyber bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet, to deliberately hurt or upset someone" DCSF 2007.

Cyber bullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated. Full details are set out in the school's behaviour, anti-bullying and safeguarding policies.

Data Protection

The quantity 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 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Handling of complaints

Members of the school community can report concerns in line with the school complaints policy and complaints of a child protection nature must be dealt with in accordance with the LA Child Protection procedures.

Appendices:

ESafety guidance for parents.

Related Policies:

Safeguarding Policy

Behaviour Policy

Anti-bullying Policy
Staff Code of Conduct
Health and Safety

Heytesbury Schools Parents' Guide to Online Safety

Research shows that the age at which children are accessing smart devices and the Internet is getting younger and younger. It's never too soon to start good ESafety habits with your child

Whether we like it or not, technology and the Internet are firmly fixed in our children's lives. Use of the Internet can be a wonderful thing, opening up new worlds and supporting children's learning and development in many ways, as well as being a fun way to relax and keep in touch with friends. However, we are all aware of the pitfalls and dangers of the online community, and since most of the current generation of parents grew up in the days before smartphones, we can feel a little clueless as to how best to protect our children. Here are some ideas which will support your primary school child's safety and well-being online.

- Set up parental controls on your home broadband and all Internet-enabled devices your child has access to.
- Password-protect all accounts.
- Choose the sites your child has access to on their account.
- Make sure your child is using child-safe search engines, such as Swiggle or KidzSearch, and activate 'safe search' options on other search engines such as Google and Youtube. (They will be taught in school to look for the green padlock)
- Switch devices to airplane mode when your child is playing online games. This will prevent them from accidentally making in-app purchases or contacting other players online.
- Pay close attention to the age ratings on games, apps and films to make sure they are suitable for your child. If you would not allow your child to watch a 15 certificate film, you should not let them play a game with the same rating.
- Set your homepage to a child-friendly one.
- Keep all devices your child will use, in a high-traffic communal area in your home, such as the kitchen or living room. Be with your child when they are online and talk about what they are doing.
- Set rules for screen time and stick to them.
- Investigate safe social media sites for kids.
- Sometimes children find themselves bullying or being bullied online (also known as 'cyberbullying'). Talk to your child about being a good friend online, and how our words and actions still hurt even if we can't see a person's reaction to them.

Talk regularly about the importance of online safety, and about what your child is getting up to online. You'll be grateful you did this, especially as your child gets older. Keeping those lines of communication open is a powerful way of letting your child know that you trust them but expect them to be honest.