ONLINE SAFETY POLICY

BUTTSBURY
PRIMARY SCHOOL
AN ACADEMY SCHOOL

Approved by:	Full Trust Board
Last reviewed on:	Summer 2024
Next review due by:	Summer 2025

At Buttsbury Primary School we create a secure and safe environment that encourages communication, self-belief, mutual respect and success. We provide a rich and balanced curriculum that develops every child, allowing them to achieve their true potential.

Our school recognises online safety issues and the potential harm and risks they can pose to children and young people. All partner agencies, stakeholders, schools and educational settings and all other organisations within the community providing services to children have a duty to understand online safety issues as part of its wider safeguarding duties; recognising their role in helping children to remain safe online while also supporting the adults who care for children.

Internet Digital and Mobile Technologies (IDMT)

Each new technology introduces new opportunities and challenges for children and young people, parents, carers and those working with young people. In order to minimise the risks involved from new technologies we need to understand how children and young people use IDMT and how this may be misused by those who may present a risk to children. It is important that we know how to respond when concerns arise.

This policy covers all technologies, platforms, hardware and software, known or unknown, at the time of its publication.

Definition of online safety

The term online safety is defined for the purposes of this document as the process of limiting the risks to children and young people when using IDMTs through a combined approach to policies and procedures, infrastructures and education.

Aims of the policy

- To raise awareness and educate staff, parents and pupils about the dangers that children and young people can face in the online world
- To promote acceptance that safety in the online world is not the removal or banning of access to digital technologies in itself but rather education and training, for both children and adults, around responsible use and potential dangers
- To ensure that our pupils recognise the risks, dangers and potential harm that may arise from the use of Internet Digital and Mobile Technologies
- To ensure that staff, pupils and parents understand how to manage these risks and potential dangers and are able to recognise, challenge and respond appropriately to any online safety concerns so that children and young people are kept safe
- To encourage staff, children and parents to consistently demonstrate safe behaviours on-line
- To develop children's self-discipline on-line
- To encourage children to cooperate with one another and with adults
- To create a positive attitude to the e-learning environment
- To work alongside parents to encourage children to develop socially, personally, academically, morally and spiritually in preparation for a positive role in online and offline societies.

Curriculum

At Buttsbury Primary School online safety education is taught with a focus on developing the knowledge and behaviours that can help children to navigate the online world safely and confidently regardless of the device, platform or app. Online safety lessons are taught explicitly and across the curriculum and include age appropriate content as set out in Education for a Connected World (UK Council for Internet Safety, 2020). Buttsbury Primary School will also take part in the annual Safer Internet Day held in February.

Risks

Children and young people do not always recognise the inherent dangers of the internet and often do not understand that online behaviour may have offline consequences.

Despite this, digital technologies can offer them opportunities to learn and develop, communicate, be creative and be entertained.

The advantages of the internet can and should out-weigh the disadvantages.

Keeping Children Safe in Education 2023 groups online safety risks into four areas: content, contact, conduct and commerce – there are sometimes known as the 4Cs of online safety.

Content
Content is anything posted online - it might be words or it could be images and video. Children and young people may see illegal, inappropriate or harmful content when online. This includes things like pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact
Contact is about the risk of harm young people may face when interacting with other users online. This includes things like peer-to-peer pressure or seeing inappropriate commercial advertising. Sometimes adults pose as children or young adults with the intention of grooming or exploiting a child or young person for sexual, criminal, financial or other purposes.

Conduct
Conduct means the way people behave online. Some online behaviour can increase the likelihood, or even cause, harm - for example, online bullying. Conduct also includes things like sharing or receiving nudes and semi-nude images and viewing or sending pornography.

Commerce
Commerce is about the risk from things like online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly. Schools should also consider how the risk from commerce applies to staff.

Use of social media by pupils

- Wider public misuse of uploaded images/videos, including potential use of mobile technology such as screen-shooting and sharing
- Sexualised images of pupils uploaded to social media websites

Forms of Abuse through Internet Digital and Mobile Technologies (IDMT)

- Children and young people have been ‘groomed’ online by adults or children and young people older than them (often pretending to be those who care) with the ultimate aim of exploiting them sexually.
- Children / young people have been bullied by other people via social networking

sites, websites, instant messaging and text messages, often known as 'cyber-bullying'.

- Inappropriate (i.e. threatening, indecent or pornographic) images of children and young people have been taken, uploaded and circulated via social network websites, mobile telephones and video broadcasting websites such as You Tube, often by other young people. This is a criminal offence under S45 of the Sexual Offences Act 2003.
- The dangers attached to gang culture can rapidly accelerate online as many gangs 'advertise' or promote themselves via websites or social networking sites or if threats of violence, threats to an individual's life or threats of retaliation are posted online by opposing gang members.
- Unsuitable websites and images can easily be accessed online.
- Images of physical abuse, crime, racism, self-harm, terrorism or physical violence may influence young minds.

Role of the school

Buttsbury Primary School takes its safeguarding duties very seriously. The school will, through a variety of strategies:

- Ensure that all staff are familiar with and exercise the school guidelines for online safety as laid out in Appendix A to this policy
- Ensure that all staff demonstrate and practice safe on-line behaviours both in and out of school
- Educate all pupils in the responsible and safe use of the internet and any and all technologies
- Ensure that appropriate levels of filtering are in place to enable safe use of the internet and monitor these
- Make children aware that uploading images of themselves online, irrespective of privacy settings, is highly dangerous and that they are putting themselves at risk
- Make children aware that such uploaded images no longer belong to them but are the property of the social media site to which they are uploading
- Make children aware that these images can be captured in a screen-shot and then shared by holders of these images through use of smart phones and other mobile technologies
- Make children over 10 aware that they are breaking the law if they upload sexualised images of themselves or others in a way that may result in them being placed on the Sex Offenders Register if convicted
- Make children aware that not all information they access on the internet is true or reliable and that it can be misleading or derogatory
- Make children aware that what they see on the internet may distort their understanding of a good, safe relationship
- Have regular liaison and update meetings with relevant agencies
- Electronic equipment taken off-site will be appropriately encrypted and stored
- Ensure that software loaded onto the system will be carried out by approved members of staff only
- Regularly update training for all staff

Role of the children

- Ensure that where inappropriate content is identified that the site is immediately closed and the member of staff in the lesson advised
- Ensure that technologies used in school are used sensibly and appropriately and that willful misuse of school or personal technology on school premises will result in withdrawal of this privilege
- Ensure that they keep themselves safe when working online and they manage the risks of internet access sensibly and in an informed way

Role of Parents

Parents can help by

- Recognising that an effective school Online Safety Policy requires close co-operation between parents, teachers and children.
- Discussing the school guidelines (set out in Appendix A to this policy) for online safety with their child, emphasising that they support this approach
- Attending Parents' Evenings and parents' functions
- Developing informal contacts with school helps to reinforce their support for the Policy.

Building on the school's existing policies

The school's Mission Statement, Behaviour Policy, Anti-Bullying Policy, Equal Opportunities Policy, Code of Conduct and Grievance Policy have very clear guidelines regarding what constitutes acceptable/unacceptable behaviour towards other people.

Monitoring and Evaluation

Policy Date: Summer Term 2024

Policy Review: Summer Term 2025

Appendix A – Guidelines on online safety

Developing filtering standards

Filters are operated and implemented by EXA according to the points below:

- It is important to use as a minimum an ISP who subscribes to the Internet Watch Foundation (IWF) filtering list. This will help to filter out some inappropriate content, but not all. Using an accredited Internet Service Provider (ISP) will also provide higher standards for filtering.
- Levels of internet access and supervision must be age appropriate and suitable for the young people. Filtering systems should be secure but adaptable.
- Older children and professionals may sometimes require temporary access to a normally restricted website in order to carry out research for a project or study. Providing this can be justified by management, restrictions may be temporarily removed; however access should be monitored.
- Access controls (filtering) fall into several overlapping types:
    - Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
    - An “allow list” restricts access to a list of approved sites. Such lists inevitably limit young people’s access to a narrow range of information.
    - Dynamic filtering examines web page content or email for unsuitable words. Filtering of outgoing information such as web searches is also required.
    - Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.
    - Access monitoring records the Internet sites visited by individual users. Attempted access to a site forbidden by the policy will result in a report.
- Management should ensure that regular checks are made to ensure that filtering methods selected are age appropriate, effective and reasonable. Access to inappropriate websites when material is perceived to be illegal must be reported to management who should inform this to the appropriate agency.

Email

Buttsbury Primary School does not allow pupils to own an internal e-mail account; *however children in Year 6 do have temporary access to a restricted account as a part of their learning in the curriculum.*

Mobile Devices

Most young people now have access to mobile telephones which are generally perceived as essential to their day to day living and communicating and now offer access to the internet, instant messaging, email, social networking, a camera and video facilities.

Mobile phones are becoming the most commonly used tool for internet access and social networking for young people. Mobile phones therefore pose one of the biggest online threats to young people as they allow instant access to all forms of IDMT.

- At Buttsbury Primary School only children in Year 6 are permitted to bring mobile phones to school. These should be turned off and kept in children’s bags.
- Children/young people and adults should be made aware to only share telephone

numbers and contact details with those known to them and ensure that electronic records (call, text and email logs) are kept of any bullying or threatening telephone calls, text messages, emails, instant messages or images received which may need to be used as evidence in any police investigation.

- Children/young people should be careful about accepting invitations to join location based social networking sites such as *TIkTok*/Snapchat that allow your location to be identified via GPS enabled phones.
- Schools and education settings and early years settings may restrict the use of mobile devices during working hours.
- Similar restrictions must apply to parents and carers when they are in the premises of the educational/early years and childcare setting.
- However, in some settings permitting responsible use of the mobile phone in conjunction with a cyber-bullying education programme is also an approach.
- Buttsbury Primary School will not scrutinise the content of a mobile device but if pupils over 10 years of age are suspected of broadcasting inappropriate or malicious content, we will not hesitate in informing parents and calling the police.

Social Networking

The Internet provides ready access to online spaces and social networking sites which allow individuals to publish un-moderated content. Social networking sites such as TikTok, Facebook, Twitter, Chat Rooms, Online Gaming Platforms and Instant Messaging can connect individuals to groups of people which may be friends in the 'virtual' world but who may have never met each other in the real world. Users can be invited to join groups and leave comments over which there may be limited or no control.

- Children/young people should be encouraged to consider the associated risks and dangers related to sending or accepting friend requests and posting personal comments, inappropriate images or videos about themselves or their peers and the subsequent difficulty in removing an inappropriate image or information once published. They should also be advised not to publish detailed private thoughts or emotions which could be considered threatening, intimidating or hurtful to others.
- Children/young people should also be encouraged to never give out any personal details or images which may identify themselves, their peers, their siblings/foster siblings, their location or any groups, schools or organisations they attend or associate with. This includes real names, dates of birth, address, phone numbers, e-mail addresses, photographs or videos, school attended, IM and email addresses, including those of friends, family / foster family and peers. This also includes any 'gangs' with which they may be affiliated.
- Children/young people must be advised about e-security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. They should be encouraged to invite known friends only and deny access to others by making their profiles private and only accept friend requests from those already known to them.
- Care should be taken to delete old and unused profiles from websites which are no longer used as these will remain accessible to others. Personal information voluntarily shared by a young person is unlikely to remain the same as the person matures and has a greater understanding of how personal information about them can impact on their later lives (i.e. prospective employers making an online search of their name and sighting inappropriate photographs, videos or content etc.).
- Professionals working or in a position of trust with children/young people (including volunteers) must also familiarise themselves about the risks and inappropriateness of sharing personal information about themselves via social networking sites with young

people. They should be made aware that any inappropriate material posted could affect their professional status.

- Professionals must responsibly restrict access to their friends and family only and 'friend requests' by a young person must be within professional boundaries.
- Professionals must also avoid social networking sites that young people are known to frequent. Under no circumstances are staff permitted to "friend" or "follow" students past or present on social networking sites until the student reached the age of 18 and where the invitation has come from the student and not from the member of staff.

Web Cam

- It is now generally accepted that the term "child pornography" should not be used, because it conflates the images of child abuse (which constitute "child pornography") with adult pornography which may be perfectly legal. There are different opinions about this, but it has now become generally accepted that the term "child sexual abuse images" is more appropriate, and most agencies have adopted this practice in their written material.
- Individuals caught in possession of child abusive images will nearly always arise as a result of a police investigation and the seizure of images, possession of which is an offence under the Protection of Children Act 1978 – amended 1994. This states:

  "It is an offence for a person….
  …. to take, or permit to be taken, or to make, any indecent photographs or pseudo-photographs of a child
  …. to distribute or show such indecent photographs or pseudo-photographs."

Multi-player games on line

Children, young people and responsible adults need to understand that their online behaviour may have consequences, as, although it's an online game, the players are real people**.**

Cyber-bullying

This section should be read in conjunction with the school's Anti-bullying policy

- 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).
- Children/young people should find using IDMT as a positive and creative part of their everyday life. Unfortunately, IDMT can also be used negatively to target a specific young person or group.
- It should also be noted that professionals, especially teachers and other education staff are particularly vulnerable to 'cyberbullying' by pupils or even ex-pupils, which may include general insults, threats, harassment, defamation, homophobic or racist remarks or other forms of prejudice based bullying. The effects of cyber bullying by young people on adults are equally distressing and the impact on the victim can be just as profound – Government guidance notes remind us that cyber bullying incidents are upsetting whoever the victim is and whatever age they are.
- Instances of cyber-bullying must be responded to sensitively and in line with existing anti-bullying policies and procedures in the organisation.
- The victim of cyber-bullying must be reassured they have done the right thing in disclosing the bullying and be supported.

Artificial Intelligence (AI) Technologies

AI is changing the way we engage with technology; it is constantly evolving and improving which can make it daunting to understand its strengths as well as its limitations. At Buttsbury Primary School we will explore the concept of AI and teach children to develop safe online behaviors in order to be informed and responsible users of all online technologies.

Committing an Illegal Act - Did You Know?

1 Receiving unsolicited emails that may contain potentially illegal material (either as an attachment or in a URL) is not an illegal offence	**4** Showing anyone else illegal material that you have received **is an illegal act**	**7** **Within 4 simple steps you could easily break the law 4 times. Each is a serious offence**
2 If you receive potentially illegal material you could easily commit an illegal act - **do not open the material or personally investigate**	**5** Printing a copy of the offensive email to report it to someone else **is an illegal act** and is classed as producing illegal material	**8** Never open unsolicited URLs or attachments. If you are suspicious that the content could be illegal report it and log that you have received it
3 Opening an attachment or URL that proves to hold illegal content **is an illegal act** and is classed as possession of illegal material	**6** Having printed a copy of the material if you give it to someone else **is an illegal act** and is classed as distributing illegal material	**9** Always report potential illegal content to the Internet Watch Foundation at www.iwf.org.uk They are licensed to investigate **you are not.**

Never personally investigate. If you open illegal content accidentally report it to your manager and IWF. Go to the IWF website and click on the report button. **Do not copy and paste the URL, write it down and type it into the reporting screen. This prevents accidental opening**. Once the email has been logged and reported to the IWF delete it from your inbox. If you are unsure, contact the IWF for advice on 01223 237 700. **The Internet Watch Foundation only deals with illegal content, please see their website for information and advice. Please note this guidance only relates to illegal content not inappropriate.**

Useful websites

Child Exploitation and Online Protection Centre
[http://www.ceop.gov.uk]

The Child Exploitation and Online Protection (CEOP) Centre aims to tackle child sex abuse wherever and whenever it happens. Part of their strategy for achieving this is to provide internet safety advice for parents and carers, training for educators and child protection professionals, and providing a 'virtual police station' for reporting abuse on the internet.

Some of these services are outlined briefly below.

Thinkuknow – online safety for young people and their parents
[http://www.thinkuknow.co.uk]

The CEOP Thinkuknow website provides a range of information on online safety for young people, with key topics including mobiles, gaming, social networking, chatting, podcasts, blogs, and peer-to-peer TV.

The content of the site is based around three key messages:

- How to have fun online
- How to stay in control online
- How to report online.

A section of the website is aimed specifically at parents and carers to try to help them understand more about what their child may be doing online.