BEESTON HILL St. LUKE'S
C of E PRIMARY SCHOOL

Online Safety Policy

Review date January 2024

Introduction

At Beeston Hill St. Luke's Primary School we are committed to ensuring that children learn how to use computers, ICT and modern technologies safely so that they:

- Are able to use ICT safely to support their learning in school
- Know how to use a range of ICT equipment safely
- Are able to use ICT and modern technologies outside school in a safe manner, including using ICT as a tool for communication
- Are prepared for the constant changes in the world of technology and understand how to use new and emerging technologies in a safe manner
- Know what to do if they feel unsafe when it comes to using technology

This policy outlines the steps the school takes to protect children from harm when using ICT and also how the school proactively encourages children to develop a safe approach to using ICT whether in school or at home.

Roles and Responsibilities

The Headteacher, alongside the E-safety officer (Matt Livesey) will:

- Ensure the policy is implemented, communicated and compliance with the policy is monitored
- Ensure staff training in e-safety is provided and updated annually as part of safeguarding training
- Ensure immediate action is always taken if any risks or dangers are identified ie reporting of inappropriate websites
- Ensure that all reported incidents of cyber bullying are investigated
- Ensure appropriate web filtering software is used to protect users from potentially damaging/offensive material

Teachers and Staff will:

- Keep passwords private and only use their own login details, which are stored securely
- Monitor and supervise pupils' internet usage and use of other IT resources
- Adhere to the Acceptable Use Agreement
- Promote e-safety and teach e-safety units as part of computing curriculum
- Engage in e-safety training
- Only download attachments/material onto the school system if they are from a trusted source
- When capturing images, videos or sound clips of children, only use school cameras or recording devices

Governors will:

- Ensure that the school is implementing this policy effectively
- Adhere to the acceptable use agreement when in school
- Have due regard for the importance of e-safety in school

Teaching and Learning

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk known as the 4Cs:

- Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial, or other purposes.
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- Commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The school will actively teach online safety at an age-appropriate level to cover the 4Cs outlined above. We recognise that online safety and broader digital resilience must be included throughout the curriculum, therefore we aim to embed online safety throughout learning whenever children are using digital devices in other lessons.

Monitoring safe and secure systems

Internet access is regulated by Schools Broadband using a filtered broadband connection which blocks access to unsuitable websites. Antivirus software has been installed on all computers and is to be maintained and updated regularly. Staff passwords are changed regularly and must be strong passwords. Staff take responsibility for safeguarding confidential data saved to laptops, i.e. use of strong passwords. If personal data has to be saved to other media, e.g. data sticks, it is to be encrypted. These procedures also comply with our GDPR policy.

The school website

- The school web site complies with statutory DFE requirements
- Images that include pupils will be selected carefully and only used if parents have given permission for such images to be posted on line.

Social Networking and Social Media

The school recognises that it has a duty to help keep children safe when they are accessing such sites at home, and to this end the school will cover such issues within the curriculum. Pupils will not access social networking sites, e.g. Facebook or Twitter in school. They will be taught about how to stay safe when using such sites at home.

Staff private use of social media:

- No reference should be made in social media to students / pupils, parents / carers / school staff or issues / situations related to the school
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Staff are not permitted to maintain a Social Media relationship with any pupil, current or alumni until such time that the pupil turns 18.

The Use of Cameras, Video and Audio Recording Equipment

Staff may only use the school's photographic or video devices to support school trips and curriculum activities. Photos should only be uploaded to the school system or school social media accounts.

Personal mobile phones and mobile devices

- Use of mobiles is discouraged throughout the school. However, mobile phones are carrid by staff in the case of an emergency i.e. lockdown.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring at the direction of the head teacher.

Management of online safety incidents

- All members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes; support is actively sought from other agencies as needed (i.e. MASH, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;

Protecting School Staff

In order to protect school staff we require that parents do not comment on school issues or staff using social networking sites. Any concerns or complaints should be discussed directly with the school.