Buckton Vale Primary School

E-Safety Policy

Introduction

E-safety is the education of children and young people on the benefits and risks of using technology. This includes the use of the internet and also other means of electronic communication such as text messages, chat rooms, social media and email.

At Buckton Vale Primary School we understand that the usage of technology is ever more prevalent in society and that E-safety is a vital part of a child's life and education in today's ever-growing digital world.

The use of digital technologies is an integral part to the lives of children, young people and adults both within the context of their daily school lives and their lives outside in the wider community. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities, to stimulate discussion, promote creativity and develop effective learning. These technologies also bring opportunities for staff to be more creative and productive in their teaching. Everyone who uses these technologies have an entitlement to safe access to the internet and digital technologies at all times.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors) who have access to and are users of school digital technology systems, both in and out of the school.

It is the duty of the school to ensure that every child and young person in its care is safe, the same 'staying safe' outcomes and principles outlined in the Every Child Matters agenda apply equally to the virtual or digital world. the Keeping children Safe in Education 2021 document sets out the legal duties that must be followed to safeguard and promote the welfare of children and young people under the age of 18 in school s and refers to online safety. This expectation also applies to any voluntary, statutory and community organisations that make use of the school's computing facilities and digital technologies.

Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its everyday practice and procedures.

Roles and responsibilities;

Headteacher and Senior Leadership Team

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety maybe be delegated to another member of the Senior Leadership Team.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher and Senior Leadership are responsible for ensuring that all staff receive suitable training to enable them to carry out their role in accordance with all safeguarding guidelines.
- Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and recording of any online safety issues

ICT management staff

Those with technical responsibilities are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and or Senior Leadership Team for investigation, action and sanctions if required
- that monitoring software and systems are implemented and updated on a regular basis.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school safety policy and practices
- they have read, understood and signed the staff acceptable use agreement
- they report any suspected misuse or problem to the Headteacher and or a member of the Senior Leadership Team.
- all digital communications with pupils, parents/carers should be on a professional level and only carried out using official school systems.
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- that pupils are monitored at all times when using digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils:

- are responsible for using the school digital technology systems in accordance with the acceptable use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related any school matters.

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet, mobile devices and any other digital technologies in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, and information about national and local online safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of on-line pupil learning and communication platforms.

This e-safety policy is intended to ensure;

Whilst guidelines and technological safeguards are very important, their use must be balanced by educating pupils to take a responsible approach. The teaching and learning of online safety and digital literacy is an essential part of any provision involving such technologies. All pupils should receive the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a fundamental focus of not only the computing curriculum but all areas of the curriculum where such technologies are employed and staff should reinforce online safety messages at all times. The teaching of online safety should be broad, relevant and provide progression, with opportunities for creative activities and provided at every possible occasion.

- Online safety should be provided as part of Computing, PHSE and other relevant lessons and revisited on a regular basis.
- Key online safety messages should be reinforced during assemblies, whole class and group activities where its impact is relevant and responsible.
- Pupils should be taught in all curriculum lessons to be critically aware of the content they access online and be guided to validate the accuracy of the information.
- Pupils should be supported in building resilience to risks posed by digital technologies such as radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision making.
- All pupils should be helped to understand the acceptable use agreement and encouraged to adopt a safe and responsible use of digital technology both in and out of school.
- Staff should act as good role models in their use of digital technologies, including the internet and mobile devices.
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of websites visited and report any breaches of online safety immediately to the Head teacher or a member of the Senior Leadership Team.

How does the school manage the use of digital technologies?

Access to the School's Network

- All staff must read and sign the Acceptable User Agreement before using any school ICT equipment
- Parents will be sent a copy of the Acceptable User Agreement and asked to read through with their child
- All users must respect the confidentiality of other users and data contained on the network as defined in current data protection legislation (GDPR)
- Machines must never be left logged on or unattended. (A machine can be locked by pressing windows key + L)
- Machines must be logged off correctly and shut down after use.
- Wireless network connection is securely password protected and monitored.
- Visiting staff/adults needing access will be given access to a guest connection only
- All users of the school network including permanent staff, children, visitors and temporary staff must first be given permission from the Headteacher or IT Manager to access the network. They will be allocated their own logons and passwords, as appropriately, which must not be shared or disclosed.
- Staff must not allow other users to access their passwords or logins.
- Software must not be installed without the consent of either the Headteacher or IT Management.
- Personal removable media (e.g. pen drives, memory sticks, CD ROM's, portable hard drives) must be password protected if they contain any school data.

Procedures for use of the internet and email

- All users must agree to and sign an Acceptable Use Agreement before access to the internet and email is permitted at Buckton Vale Primary School.
- Parents are informed that pupils will be provided with supervised internet access.
- Users must access the internet and email using their own logon/password and not attempt those of another individual.
- All passwords must remain confidential to the user and must not be shared.
- Internet and email filtering software is installed in line with Ofsted's filtering and monitoring statutory guidance.
- Personal email or messaging between staff, pupils and or parents/carers must not take place.
- All staff and pupils will be provided with a school email account.
- Approved email accounts provided by school ending with @bucktonvale.tameside.sch.uk must only be used for teaching and learning associated with school and not for personal communication.
- Pupils and staff may only use approved email accounts on the school system.
- School will ensure that the use of internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critical aware of the materials they are shown and how to validate information before accepting its accuracy.
- If staff or pupils discover unsuitable sites, the URL, time and content must be reported to the Head teacher or a member of the Senior Leadership Team and recorded on CPOMs. This will be investigated and appropriate action taken, liaising with the broadband provider and, if necessary, reported to the appropriate authorities.
- Internet and email use will be monitored regularly by the IT Management company as outlined in the acceptable user agreement.

Social networking and chat rooms

- At Buckton Vale we block/filter access to social networking sites unless a specific use is approved.

- Through quality E-safety education children are taught about social media platforms and rules such as age restrictions for access, security/privacy and SMART rules.
- Class Dojo and Tapestry sites will be used by staff and parent/carers to communicate and share class and school information, news, photos and written observations. Access is controlled with secure passwords. These sites will be used in the event of remote learning.
- Pupils will not access social networking sites e.g. 'Meta (Facebook)', 'Twitter', 'Instragram', 'Tic Tok', 'snapchat', whilst at school.
- Pupils will be taught the importance of personal safety when using any social networking sites and chat rooms, games sites, newsgroups or other communication apps.
- Pupils will be advised to use nick names and avatars when using any form of social networking as opposed to using their personal information or image.
- Pupils will be advised to never give out personal details of any kind which may identify them or their location.
- Pupils will be advised not to place personal photos on any social networking space.
- Pupils will be advised on security and encouraged to set passwords, deny access to unwanted individuals and instructed how to report and block unwanted communications.
- Pupils will not be allowed to access public or unregulated chat rooms
- Pupils will only be allowed to use regulated educational chat environments for specific curriculum learning and use will be supervised.
- Staff guidelines are clearly communicated and annual training provided as stated in the acceptable user agreement.
- Staff members will not communicate with pupils or parent/carers through personal social networking accounts.
- In line with the acceptable user agreement staff will not publish any comments, photos or videos which could cause a negative impact to the school's reputation or the reputation of any pupil, staff member, governing board, parent/carer, volunteer or member of the local community.

Procedures for use of cameras, video equipment and webcams

- Permission will be obtained from a pupil's parent/carer before photographs and video footage can be taken.
- Permission will be obtained from staff and visitors before photographs or video footage can be taken.
- All photographs and video footage will be saved into a secure area, accessible only to authorised members of staff.
- Any adult using their own camera, video recorder during a trip or visit must first gain permission from the Head teacher to use their own equipment. All pictures and videos should be saved to the school system by the end of the working day and not left on a personal device.
- Personal mobiles phones with cameras must not be used by a member of staff under any circumstances.
- Photographs and video footage stored will be deleted once the children/adults are no longer associated with the school.

Photographs taken by parents/carers for personal use

- The school will ensure that parents are aware of their responsibilities. This will be done by announcing before the event, to remind parents that, any photographs or video footage taken are for private use and retention only and are not for publication in any manner including personal websites or social networking site.

Procedures to ensure safety of the Buckton Vale's Website

- All content published to the Buckton Vale Primary School website will be carefully monitored and approved by the Head teacher and Senior Leadership Team to ensure suitability and compliance with policies and parental consents. This is subject to frequent checks to ensure that no material has been inadvertently uploaded, which might put pupils and staff at risk.

Procedures for using mobile phones

- Pupils are not permitted to carry or use mobile phones, smart phones or PDA's at any time during school hours. These must be handed into the school office on arrival and collected at the end of the day. Any device discovered will be kept by the Headteacher; she will then be responsible for its safety, return and resulting sanctions.
- Staff are not permitted to use their phones during teaching time. Mobile phones must be kept on silent and always stored away from view during teaching hours.
- Staff who use personal mobile phones to access their school email must ensure that their device is encrypted with a personal password, pin or fingerprint recognition.
- Passwords and personal information related to personal devices should be kept confidential.

Procedures for using wireless games consoles/portable media players

- The use of wireless games consoles/portable media players is not permitted at any time at Buckton Vale Primary School unless the activity is supervised by an authorised adult.
- Staff may use portable media players only in an educational context e.g. when appropriate to a specific lesson such as music for a PE session or after school club during teaching time.

Introducing acceptable use to pupils

- Rules for internet access will be shared with all pupils during any teaching and learning sessions where digital technologies are used.
- Responsible internet use, covering both school and home use, will be included in the PSHE and Computing online safety curriculum.
- An annual Safer Internet Day will be held in school to further develop awareness of e-safety amongst pupils.
- E-safety will be a key part of the curriculum that is flexible, relevant and engages interest. The Computing curriculum will be used to promote E-safety and digital literacy through teaching pupils to be resilient and develop the skills to protect themselves from harm; taking responsibility for their own and others safety.
- Pupils will be taught the appropriate skills to stay safe before being allowed access to the internet and be reminded of the rules and risks before any lesson which includes access to the internet.
- Pupils will be informed that use of the internet is closely monitored and misuse will be dealt with appropriately.

Assessing risks and E-Safety complaints

- As a school we will take all reasonable precautions to ensure that all users access only appropriate materials in an appropriate manner. However due to the international scale and linked nature of the internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. If such an event occurs opportunities are taken to use this as a teaching tool to show the dangers of the internet and how to deal with them in an appropriate manner.
- All staff and children are made aware that the internet and device usage will be monitored regularly and can be traced to an individual user; action will be taken if inappropriate use is discovered.
- Deliberate access to inappropriate material or misuse of school technology and equipment will be dealt with in line with the sanctions detailed below.

- A laptop issued to staff or children remains the property of the school and users should therefore refer to the laptop agreement for use both in and out of school hours both at home and school.
- Complaints of a child protection nature will be dealt with in accordance with the school child protection policy.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.
- The Head teacher will ensure that the E-Safety Policy is implemented and compliance with the policy is monitored.

Sanctions to be imposed if procedures are not followed

- Any breach of this policy for pupils will result in sanctions most appropriate to the offence, these will include
    - Immediate removal from the computer, internet, equipment being used.
    - Letter sent home/parents informed
    - Discussions with class teacher/headteacher, and possible suspension of school equipment for a period of time.

- Any breach of this policy for staff/adults will result in sanctions most appropriate to the offence, these will include
    - Immediate removal from the computer, internet, equipment being used.
    - Discussions with Headteacher, and possible suspension of school equipment for a period of time.
    - Disciplinary action and reporting to headteacher, chair of governors and/or to Tameside MBC internal auditing department.
    - Details may be passed to police in more serious cases.
    - Legal action will be taken in more extreme circumstances which may result in dismissal.

The procedures in this policy are subject to ongoing review and modification in order to keep up with advances in technology.

Signed (Headteacher) _____ Date _____

Signed (Chair of Governors) _____ Date _____