Budbrooke Primary School

Online Safety Policy

Date adopted by Governors:	**16th December 2021**
Date for policy review:	**November 2021**
Person responsible for review:	**Head Teacher**

1. Introduction

At Budbrooke Primary school, we understand the responsibility we have to educate our pupils on online safety issues; teaching them appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. We have a whole school approach to the safe use of ICT and creating this safe learning environment includes three main elements:

- an effective range of technological tools
- policies and procedures, with clear roles and responsibilities
- a comprehensive online safety programme for pupils and staff

Online safety encompasses Internet technologies and electronic communications such as mobile phones and tablets as well as collaboration tools, use of Social Media and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Writing and reviewing the Online safety policy

- The Online Safety Policy has been written by the Computing coordinator after consultation with the Headteacher, school staff and governors.

- The Online Safety Policy will be reviewed annually and compliance will be monitored throughout the year.

Why Internet use is important

- The Internet is an essential element in 21st century 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.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- 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 in an online world.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

2. Statement of Intent

The purpose of this policy is to ensure that all staff, parents, governors and children at Budbrooke Primary school understand and agree the school's approach to online safety. Budbrooke's online safety policy operates in conjunction with other policies including those for Safeguarding, Behaviour, Anti-Bullying, Data Protection, Code of Conduct policy and Acceptable Use.

3. Aims and Objectives

It is the aim of this school to provide every child with the best education possible. Our objective in setting out the school's Online Safety Policy is to make everyone aware that we want all pupils to benefit as fully as possible from the education provided safely within the school by:

4. Teaching and Learning

- Having a relevant up-to-date online safety curriculum which is progressive from Early Years to the end of Year 6.
- A curriculum that is threaded throughout other curriculums and embedded in the day-to-day lives of our pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Pupils are taught about the safe use of social networking sites as part of their online safety lessons in school
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Training for staff and governors which is relevant to their needs and ultimately positively impacts on the pupils.
- Scheduled pupil voice sessions and learning walks steer changes and inform teaching and learning requirements.
- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Online safety rules will be discussed with the pupils at the start of each year and in line with the units set out in the Computing Scheme of Work.
- Pupils will be taught how to use communication tools appropriately, as part of general ICT/Computing lessons and online safety lessons.

5. Communication

- Through our home/school links and communication channels, parents are kept up to date with relevant online safety matters, policies and agreements. They know who to contact at school if they have concerns.
- Online safety posters will be prominent in environments such as the Computing Suite, so all users can see them.
- Pupils, staff and parents have Acceptable Use Policies which are signed.

6. E-mail content and the school website

- Pupils may use a school email account in the school when supervised and for an educational purpose.
- The contact details on the school website should be the school address, email and telephone number, staff or pupils' personal information will not be published.
- Photographs that include pupils will be selected carefully and only if permission from parents and carers has been granted.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media

7. Social networking and personal publishing

- The school will deny access to social networking sites and children will be strongly advised not to use these at home in line with the Terms of Use linked to each service.
- Reminders will be shared with parents through the school newsletter and in weekly class emails.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils, and that many social networking sites have a specified minimum age of 13 years old.

8. Filtering and monitoring

- The school will work with the LA, Academy Trust, DfE and Internet Service Provider (ISP) to ensure systems to protect pupils are reviewed and improved. School ICT systems capacity and security are regularly reviewed through ongoing monitoring via the Local Authority.
- If staff or pupils discover an unsuitable site, it must be reported to Senior Leadership Team/Computing Subject coordinator.

- An incident log must also be completed on our schools Behaviour Log system if a pupil has been found to be misusing our computing system.
- Our online safety policy clearly states how monitoring of online safety is undertaken and any incidents/infringements to it are dealt with.
- Pupils are informed that network and Internet use is monitored and misuse is followed up.

9. Assessing Risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. Our 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. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- Emerging technologies will be examined for educational benefit before any potential use in school is allowed.
- Curriculum Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.
- 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, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can take this request to the Computing Coordinator who can request that these sites be temporarily or permanently removed from the filtered list
- Rules for Internet access will be posted in all networked rooms.

10. Handling online safety complaints

- The Headteacher will deal with complaints of Internet misuse. They may seek advice and guidance from the school Computing Subject coordinator and designated safeguarding leads.
- Any complaint about staff misuse must be referred to the Headteacher
- Complaints of a child protection nature must be dealt with in accordance with the school Safeguarding & Child Protection Policy.

11. Infrastructure, system security, filtering and monitoring

- The security of the school information systems will be reviewed regularly
- Virus protection will be installed and updated regularly
- The school uses the Warwickshire Broadband with its firewall and filters.
- The school provides an additional level of protection through its deployment of Policy Central in partnership with Warwickshire ICT Development Services
- The school will work in partnership with the Warwickshire ICT Development Service to ensure filtering systems are as effective as possible
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the Headteacher or the Computing coordinator, who will report this to the ICT Development Service filtering team.
- All users will have clearly defined access rights to school ICT systems. The Local Authority ICT Development Service provides the school with ICT Equipment where access rights are already defined.
- Social networking sites and newsgroups will be blocked to pupils unless a specific use is approved.
- Staff will monitor the usage of the communication tools by pupils in all areas, in particular message and communication tools and publishing facilities.

12. Usernames and passwords

- All pupils will be provided with a username and password which will provide them secure access to school curriculum devices, the School website and email at an age appropriate level.
- Pupils in Reception will log on with a class account.
- Use by pupils in this way should always be supervised and members of staff should never use a class log on for their own network access.
- All pupils new to the school are initially provisioned with a username and password that is unique to them
- All Staff will be provided with a username and password which will provide them secure access to school curriculum devices, the school website and email.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- 'Guests' such as supply teachers are provided with a username and password if they require access to school systems. The School Office record this to make it possible to trace back any instances if misuse.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

13. Personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data. Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, USB stick or any other removable media, the data must be encrypted and password protected

14. Communications (Email/Blogging)

- Pupils are taught how to use email accounts safely from Year 1 onwards
- Pupils may only use approved we-learn e-mail accounts on the school system.
- Children are not allowed access to other e-mail accounts whilst in school.
- Pupils are taught about the appropriate use of email/blogging, including the type of language that they use in different situations
- Pupils are taught to tell an adult they trust if they receive an offensive e-mail/blog.
- Pupils are taught not reveal personal details of themselves or others in e-mail/blog communication, or arrange to meet anyone without specific permission
- The forwarding of chain letters is not permitted.
- Access to online blogging systems will need to be pre-approved by the Senior Leadership Team.
- Any concerns with blogging content may be recorded and dealt with in the following ways:
    - a) The user will be asked to remove any material deemed to be inappropriate or offensive.
    - b) The material will be removed by the site administrator if the user does not comply.
    - c) Access to the communication tool for the user may be suspended.
    - d) The user will need to discuss the issues with a member of SLT before reinstatement.
    - e) A pupil's parent/carer may be informed.

15. Video conferencing

- Video conferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- External IP addresses will not be made available to other sites.

- Pupils should ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing will be supervised appropriately for the pupils' age.
- Teaching staff and pupils will only use video conferencing approved tools, such as Microsoft Teams
- When communicating with pupils, staff will only use online systems or apps approved by the Senior Leadership Team.

16. Mobile phones

- Pupils are not allowed access to mobile phones in school, unless there has been a specific agreement with a parent for a specific reason
- Mobile phones will not be used by staff during face-to-face sessions with pupils
- The sending of abusive or inappropriate text messages between any members of the school community is forbidden.
- Staff contact with pupils via a mobile phone is forbidden
- Staff will be made aware that connecting a personal mobile phone / Smart phone to the school's wireless system will result in that phone being monitored in the same way that networked devices are monitored.

17. Cyberbullying

Cyberbullying (along with all forms of bullying) will not be tolerated in school and there are clear procedures in place to support anyone affected by Cyberbullying.

- All incidents of Cyberbullying reported to the school will be recorded.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary

Sanctions for those involved in Cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended at school for the user for a period of time.
- Parent/carers may be informed.
- The Police will be contacted if a criminal offence is suspected.

18. Unsuitable / Inappropriate activities

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Promotion or conduct of illegal acts, e.g. under child protection, obscenity, computer misuse and fraud legislation.
- Criminally racist material in the UK
- Child sexual abuse images
- Pornography
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred
- Threatening behaviour, including promotion of physical violence or mental harm
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- Using school systems to run a private business
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Warwickshire ICT Development Service / the school

- Revealing or publicising confidential information (e.g. personal information, databases, computer/network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic that causes network congestion and hinders others in their use of the internet
- On-line gambling

19. Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

- Complaints of Internet misuse will be dealt with by the Headteacher or Deputy Headteacher
- Complaints of a child protection nature must be dealt with in accordance with the school's Safeguarding and Children Protection Policy.
- If any apparent or actual misuse appears to involve illegal activity then the school will report the incident to the Local Authority in the first instance and inform the police.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

Inappropriate usage by Pupils includes:

- Deliberately accessing or trying to access material that could be considered illegal
- deliberately accessing or trying to access material that is not age-appropriate
- Unauthorised use of non-educational sites during lessons
- Unauthorised use of mobile phone / digital camera / other hand-held devices
- Unauthorised use of social networking / personal email
- Attempting to access or accessing the school network using another users account
- Sending an email, text or other electronic message that is regarded as offensive, harassment or of a bullying nature
- Actions which could bring the school into disrepute or breach the integrity or ethos of the school.

Depending on the serious of the inappropriate usage by a pupil, staff will use one or more of the following sanctions:

- Verbal warnings
- Refer to the Headteacher/Deputy Headteacher
- Inform parents/carers
- Remove network/internet access rights
- Refer to the police

Inappropriate usage by Staff includes:

- Deliberately accessing or trying to access material that could be considered illegal
- Excessive or inappropriate personal use of the internet/personal email/social networking sites/instant messaging
- Sharing username and passwords with others in order to allow them to access school systems
- Careless use of personal data e.g. transferring data in an unsecure manner
- Deliberate actions to breach data protection or network security rules
- Sending an email, text or other electronic message that is regarded as offensive, harassment or of a bullying nature
- Using personal email/social networking/instant messaging to carry out digital communications with pupils
- Actions which could compromise the staff members' professional reputation
- Actions that could bring the school into disrepute or breach the integrity of the ethos of the school

- Deliberately accessing or trying to access offensive or pornographic nature
- Breaching copyright or licensing regulations

Depending on the serious of the inappropriate usage by a member of staff the Headteacher/Deputy Headteacher may use one or more of the following sanctions:

- Refer to the Local Authority/ICT Development Service or HR
- Refer to Technical Support staff for action re: filtering
- Disciplinary action
- Refer to police

20. Responsibility for the Policy and Procedure

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Role of the Governing Body

The Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports.

A member of the Governing Body has taken on the role of Online safety Governor. The role of the Online safety Governor will include:

- regular communication/meetings with the Computing coordinator or Designated Safeguarding Lead
- reporting to relevant Governors committee / meeting
- attending relevant training
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs

Role of the Head Teacher and SLT

The Head Teacher will:

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Computing coordinator.
- The Headteacher / Senior Leaders are responsible for ensuring that the Computing coordinator and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive regular monitoring reports from the Computing coordinator at Senior Leadership meetings.

Role of the Computing Coordinator

The Computing Co-ordinator will:

- take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies or documents
- works alongside the Designated Safeguarding Leads to ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Designated Safeguarding Lead, Local Authority, ICT technician or any other relevant body in relation to online safety
- receives reports of online safety incidents and a log of incidents to inform future online developments.

- meets regularly with the Safeguarding team to discuss current issues, review incident logs and filtering or change control logs
- attends relevant meetings of Governors where an update of on online safety is required
- reports regularly to the SLT

Role of the Network Manager/Technical staff:

The ICT Technician, Headteacher and Computing coordinator 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 Academy Trust, Local Authority or other relevant body Online Safety Policy or 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 is implemented and managed by Warwickshire County Council's broadband service.
- that all staff involved with school security of the network keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update staff as relevant
- that the use of the network, internet, shared files, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher
- that monitoring software and systems are implemented and updated as agreed in our policies

Role of Teaching and Support staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current Online safety Policy and practices
- they have read, understood and signed the Staff and Volunteer Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher/ Senior Leadership Team/Computing subject coordinator for investigation, action and consequences
- all digital communications with pupils and 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 and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- processes are in place for dealing with any unsuitable material that is found during internet searches and where internet use is pre-planned pupils should be guided to sites checked as suitable for their use

Role of the Designated Safeguarding Lead

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious child protection or safeguarding issues to arise from:

- sharing of personal data
- access to illegal or inappropriate materials
- inappropriate on-line contact with adults or strangers
- potential or actual incidents of grooming
- cyber-bullying
- extremism and radicalisation

Role and Rights of Pupils

Pupils are responsible for:

- using the school's digital technology systems in accordance with the Pupil Acceptable Use Policy
- 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 the school's policies on the use of mobile devices and digital cameras.
- they should also know and understand the school's policies on the taking or use of images and on cyber-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 to their membership of the school

Role and Rights of Parents

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet or mobile devices in an appropriate way. Our school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national or 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 the website and any on-line pupil records

20. Raising Awareness of this Policy

We will raise awareness of this policy via:

- the school website
- annual safeguarding update training
- meetings with parents such as introductory, transition, parent-teacher consultations and periodic curriculum workshops
- school events
- meetings with school personnel
- communications with home such as weekly newsletters and of start of half term newsletters
- reports such as annual report to parents and Head Teacher reports to the Governing Body
- information displays in the main school entrance

21. Training

We ensure all school personnel have equal chances of training, career development and promotion.

Periodic training will be organised for all school personnel so that they are kept up to date with new information and guide lines concerning online safety.

22 Evaluation and Review

The effectiveness of the online safety provision provided by the school will be undertaken annually by the Governing Body and reported to parents in the Annual Governors Report. A review of the Online Safety Policy document is undertaken every year. The Online Safety Policy is a working document and is kept under constant review.