Battle Primary Academy
E-Safety Policy

Written By:	NETAT
Agreed by	BPA Local Governing Body
Review Date	January 2020

1.0 - Introduction

1.1 - The resources used by pupils in Battle Primary Academy are carefully chosen by the teacher and determined by curriculum policies. Use of the Internet, by its nature, will provide access to information which has sometimes not been selected by the teacher.

1.2 - Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at times they will be able to move beyond these to sites unfamiliar to the teacher. There is therefore the possibility that a pupil may access unsuitable material either accidentally or deliberately.

1.3 - The purpose of this policy is to:

- Establish the ground rules we have in school for using the internet;
- Describe how these fit into the wider context of our behaviour and PHSE policies;
- Demonstrate the methods used to protect the children from sites containing unsuitable material.

1.4 - The Academy believes that the benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one that we share with parents and carers.

1.5 - At Battle Primary Academy we feel that the best recipe for success lies in a combination of site-filtering, of supervision and by fostering a responsible attitude and informed approach to the internet in our pupils in partnership with parents and carers.

1.6 - Parents will be sent an explanatory letter and the rules, which form our Pupil Internet Agreement (Annex 2), as part of our welcome pack. We will also aim to disseminate any relevant published materials to parents.

2.0 - Teaching and Learning

2.1 - Use of the Internet in Teaching and Learning

2.1.1 - 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 academy's management functions.

2.1.2 - We use the internet for a number of reasons:

- Internet use is part of the statutory curriculum and a necessary tool for learning;
- The internet is a part of everyday life for education, business and social interaction;
- The academy has a duty to provide quality internet access as part of teaching and learning;
- Pupils use the internet widely outside school and need to learn how to evaluate internet information and to take care of their own personal safety and security whilst online.

2.1.3 - The benefits of using the internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- Educational and cultural exchanges between pupils worldwide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across networks of schools, support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Access to learning wherever and whenever convenient.

2.2 - Use of the Internet to Enhance Learning

2.2.1 - The Academy's internet access will be designed to enhance and extend education.

2.2.2 - Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for internet use.

2.2.3 - The Academy will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

2.2.4 - Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity.

2.2.5 - Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

2.2.6 - Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

2.3 - Learning to Evaluate Internet Content

2.3.1 - As with many media sources, information received via the internet, email or text message requires strong information handling and digital literacy skills in order to determine quality and reliability.

2.3.2 - In particular, it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. Pupils will be taught to identify, where possible, the origin of materials they read and shown how to validate information before accepting its accuracy.

2.3.3 - Pupils will be taught to critically evaluate content found on the internet, taking into account the reliability of the source and potential bias.

2.3.4 - The evaluation of online materials is a part of teaching and learning in every subject.

3.0 - Managing Information Systems

3.1 - Maintaining Information Systems Security

3.1.1 - Virus protection will be updated regularly.

3.1.2 - Personal data sent over the internet will be encrypted.

3.1.3 - Portable media may not used without specific permission followed by a virus check.

3.1.4 - Unapproved software will not be allowed in pupils' work areas or attached to email.

3.2 - Managing Emails

3.2.1 - Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

3.2.2 - Access in school to external personal email accounts may be blocked.

3.2.3 - The forwarding of chain messages is not permitted.

3.2.4 - Staff should only use school email accounts to communicate with pupils as approved by the Senior Leadership Team.

4.0 - Managing Published Content

4.1 - We have created a website that inspires pupils to publish work of a high standard.

4.2 - We use the website to celebrate pupils work, promote the school and publish resources for projects.

4.3 - Publication of information will be considered from a personal and school security viewpoint.

4.4 - The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.

4.5 - The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate and editorial guidance will help reflect the academy's requirements for accuracy and good presentation.

4.6 - The website will comply with current guidelines for publications including respect for intellectual property rights and copyright.

4.7 - Publishing Pupil's Images or Work

4.7.1 - Still and moving images and sounds add liveliness and interest to a website, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount.

4.7.2 - The publishing of pupils' names with their images is not acceptable, since published images could be reused, particularly if large images of individual pupils are shown.

4.7.3 - Images of a pupil will be published unless parents request otherwise. Pupils also need to be taught the reasons for caution in publishing personal information and images online.

4.7.4 - Pupils' full names will not be used anywhere on the website in association with a photograph.

4.8 - Managing Social Networking, Social Media and Personal Publishing

4.8.1 - Parents / carers and teachers need to be aware that the internet has emerging online spaces and social networks which allow individuals to publish unmediated content.

4.8.2 - Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

4.8.3 - Although primary age pupils should not use Facebook, Instagram, Snapchat or similar sites, pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

4.8.4 - No member of staff should use social networking sites or personal publishing sites to communicate with students, past or present.

4.8.5 - Staff need to be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Examples include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

4.8.6 - Academy staff must not, under any circumstances make reference to pupils or Academy business on any social media The Academy will control on-site access to social media and social networking sites.

4.8.7 - From years 1 and above, pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends / family, specific interests and clubs etc.

4.8.8 - From years 1 and above, pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.

4.8.9 - Staff are advised not to run social network spaces for pupil use on a personal basis.

4.8.10 - Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

4.9 - Managing Filtering

4.9.1 - The Academy will work with its ICT consultant to ensure that systems to protect pupils are reviewed and improved.

4.9.2 - If staff or pupils discover unsuitable sites, the URL must be reported to the ICT Technician or a senior member of staff.

4.9.3 - The Academy's broadband access includes filtering appropriate to the age and maturity of pupils. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

4.9.4 - Any material that staff believe to be illegal must be reported to the Head Teacher, who will inform the appropriate agencies.

4.9.5 - We will keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies. There are dangers for staff, however, if personal phones are used to contact pupils or families and therefore this will only be done when authorized by a senior member of staff.

4.9.6 - The sending of abusive or inappropriate text, picture or video messages is forbidden. Abusive messages should be dealt with under the Academy's behaviour policy.

4.9.7 - Emerging technologies will be examined for educational benefit and the Head Teacher, in consultation with staff, will give permission for appropriate use.

4.9.8 - Mobile phones will not be used during lessons or formal school time.

4.9.9 - Pupils are not allowed to bring mobile phones into school. Under certain circumstances exceptions can be discussed with the Head Teacher, so that pupil mobile phones can be kept in the school office. Parents must complete the permission slip to acknowledge that the school takes no responsibility for phones which are left in the office.

5.0 - Policy Decisions

5.1 - Authorising Internet Access

5.1.1 - We allocate internet access for staff and pupils on the basis of educational need. It should be clear who has authorised internet access and who has not.

5.1.2 - Authorisation is granted on an individual basis and usage is fully supervised. Normally all pupils will be granted internet access.

5.1.3 - Parental permission is required for internet access in all cases as new pupils join the Academy.

5.1.4 - All staff must read and sign the Acceptable Use Policy**.**

5.1.5 - At Key Stage 1, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved online materials.

5.2 - Assessing Risks

5.2.1 - Battle Primary Academy will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the Academy nor NET Academies Trust can accept liability for the material accessed, or any consequences resulting from internet use.

5.2.2 - The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly and after every breech of this policy.

5.3 - E–Safety Complaints

5.3.1 - Complaints of internet misuse will be dealt with under the Academy's Complaints Procedure.

5.3.2 - Any complaint about staff misuse must be referred to the Head Teacher. If the complaint is about the Head Teacher this should be reported to the Chair of Governors.

5.3.3 - All e–Safety complaints and incidents will be recorded by the Academy — including any actions taken.

5.3.4 - Pupils and parents will have access to the Academy's Complaints Policy. Parents and pupils will work in partnership with staff to resolve issues.

5.3.5 - Discussions will be held with the police and/or Local Authority Safeguarding Children Board to establish procedures for handling potentially illegal issues.

5.3.6 - Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

5.4 - Internet Use Across the Community

5.4.1 - We recognise that children can access the internet outside of school, and offer support and advice to parents on internet safety though regular information sent home with children and through advice on our website.

5.4.2 - The school will be sensitive to internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

5.4.3 - We also hold an E-safety workshop for parents / carers annually. This is for parents of children from Year 1 to Year 6.

5.5 - Cyberbullying

5.5.1 - Cyberbullying is defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone", DCSF 2007.

5.5.2 - It is essential that pupils, Academy staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse.

5.5.3 - Promoting a culture of confident users will support innovation and safety. DCSF and Childnet have produced resources and guidance that will be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying

5.5.4 - Cyberbullying (along with all forms of bullying) will not be tolerated in school. All incidents of cyberbullying reported to the Academy will be recorded and dealt with in accordance with the Behaviour Policy.

5.5.5 - There are clear procedures in place to investigate incidents or allegations of cyberbullying:

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

5.5.6 - Sanctions for those involved in cyberbullying may include:

- The perpetrator 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;
- Parents / carers will be informed and the Police will be contacted if a criminal offence is suspected.

5.6 - Anti-radicalisation

5.6.1 - Many extremist groups, such as far right groups, animal rights activists and Islamic fundamentalists, who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts.

5.6.2 - Because of their personal circumstances, some young people may be susceptible to these influences.

5.6.3 - Battle Primary Academy takes its responsibility under the Prevent Duty to safeguard children against radicalisation and radical ideologies very seriously and will not tolerate extremism in our school.

5.6.4 - Staff need to be vigilant against such content and particularly aware of those young people who may be vulnerable to harmful influences from extremists via the internet. All staff will receive adequate training, as outlined in the Academy's Safeguarding Policy.

5.6.5 - Under the Academy's Pupil Internet Agreement (Annex 2), content promoting any extremist group is considered to be 'offensive material' and it is accordingly forbidden for pupils to deliberately access such content.

5.6.6 - Suitable filtering systems will be in place to prevent children from accessing terrorist and extremist material, with a review of filtering taking place periodically and whenever there is any incident of a young person accessing websites advocating violent extremism.

5.6.7 - The Nominated Safeguarding Officer will record and review all incidents in order to establish whether there are any patterns of engagement with extremist groups.

5.6.8 - The Academy's Safeguarding Policy outlines the steps that the Academy will take to pro-actively safeguard children against harmful influences from extremists and the process for handling concerns about any child who is thought to be at risk from such groups.

5.7 - Other e-Safety Issues

5.7.1 - Sexting – Children in Year 5 and 6 will be informed about the implications of sexting and how, once a picture has been sent, this image can never fully be removed from the internet.

5.7.2 - Pornography – children may come across some type of pornographic content when searching the internet. Children are taught about what to do if they come across this type of material and who to speak to.

5.7.3 - Websites advocating extreme or dangerous behaviours - some internet sites advocate dangerous activities such as self-harming, suicide, anorexia or substance misuse. Battle Primary Academy aims to create a safe space for the open discussion of these and other issues and staff will be vigilant against children accessing such sites.

6.0 - Communication Policy

6.1 - Communicating this Policy to Pupils

6.1.1 - At Battle Primary Academy we teach about e-safety as an ICT lesson activity and as part of every subject whenever pupils are using the internet.

6.1.2 - All users are informed that network and internet use will be monitored.

6.1.3 - Pupil instruction in responsible and safe use should precede internet access every time they go online.

6.1.4 - Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.

6.1.5 - We will use high quality and up to date e–safety programmes in our e-safety teaching.

6.1.6 - Communicating this Policy to Staff

6.1.7 - The e–Safety Policy will be formally provided to and discussed with all members of staff and published on the school website.

6.1.8 - To protect all staff and pupils, the school will implement Acceptable Use Policy (Annex 1). Staff should be aware that internet traffic can be monitored and traced to the individual user; discretion and professional conduct is essential.

6.1.9 - Staff training in safe and responsible internet use will be provided.

6.2 - Parental Support

6.2.1 - Parents' attention will be drawn to the Academy's e–Safety Policy in newsletters and on the Academy website.

6.2.2 - A partnership approach with parents will be encouraged. This may include parent meetings with demonstrations and suggestions for safe home internet use.

6.2.3 - Parents will be requested to sign a Pupil Internet Agreement as part of the Academy's on entry procedures. Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.

7.0 - Policy Management

7.1 - This policy is linked to the following Academy policies: Safeguarding and Child Protection, Whistle Blowing, Health and Safety, Behaviour and Anti-Bullying, Home School Agreements, ICT and PHSE Curriculum**.**

7.2 - Approval and Review

7.2.1 - This policy was approved by the Board on August 2015

7.2.2 - This policy shall be reviewed no less than once every two years to ensure its continued effectiveness and compliance with the law and regulations.

7.2.3 - Next review date: January 2020

ANNEX 1 Staff Agreement Form
Covers use of digital technologies in school: i.e. email, internet, intranet and network resources, learning platform, software, equipment and systems.

Acceptable Use Policy (AUP): Staff Agreement Form

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / internet / intranet / network, or other school / Trust systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business.
- I will only use the approved school email or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not download any software or resources from the internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended antivirus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.

ANNEX 1 Staff Agreement Form

Covers use of digital technologies in school: i.e. email, internet, intranet and network resources, learning platform, software, equipment and systems.

- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.
- I understand that all internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Agreement

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I wish to have an email account; be connected to the Intranet & internet; be able to use the school's ICT resources and systems.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

School .....

Head Teacher Authorisation

I approve this user to be set-up.

Signature ..... Date .....

Full Name ..... (printed)

ANNEX 2 – Internet Agreement

All pupils and their parents / guardians will be asked to read and sign an agreement covering the expectations we have of pupils using the internet in school.

Battle Primary Academy Pupil Internet Agreement

This is to be read through with your parent(s) and then signed. You will be allowed internet Access after this is returned to school.

- At Battle Primary Academy, we expect all pupils to be responsible for their own behaviour on the internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.

- Pupils using the internet are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher.

- Pupils are expected not to use any rude language in their email communications and contact only people they know or those the teacher has approved. It is forbidden to be involved in sending chain letters.

- Pupils must ask permission before accessing the internet.

- Pupils should not access other people's files unless permission has been given.

- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.

- No program files may be downloaded to the computer from the internet.

- No programs on disc or CD Rom should be brought in from home for use in school.

- Homework completed at home may be brought in on USB key but this will have to be virus scanned by the class teacher before use.

- Personal printing is not allowed on our network for cost reasons (e.g. pictures of pop groups/cartoon characters).

- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.

- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to internet resources.

I have read through this agreement with my child and agree to these safety restrictions.

Signed:_____(Parent/Responsible Adult)

Name of child: _____