ALBOURNE C.E. PRIMARY SCHOOL

Internet Use and E-Safety Policy

'On our learning journey together'.

The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to e-safety. The strategies are based on: managing access, developing responsibility and safe use of the Internet and to enhance learning.
It should be read in conjunction with other associated policies.

Introduction

Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing what is now regarded as an essential role in the everyday lives of children, young people and adults. Consequently, schools need to ensure children are properly equipped with the skills to access IT and promote life-long learning and future economic well-being.
Computing covers a wide range of resources, including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of IT within our society as a whole. Currently, the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other devices with web functionality

Whilst exciting and beneficial, both in and out of the context of education, users need to be aware of the range of risks associated with the use of these Internet technologies.
As a school we understand the responsibility to educate our pupils in e-Safety issues, teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.
This policy is inclusive of both fixed and mobile internet.

Why is Internet access important?

- The purpose of the Internet in school is to raise educational standards of pupils and support the professional work of all staff.
- It is an entitlement for students to allow them to develop the necessary skills for living in a technological society.
- Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access as it is an essential part of education in this current world.
- Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

What are the benefits to the School?

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries
- Access to appropriate child friendly resources and information e.g. Espresso
- Educational and cultural exchanges between pupils world-wide
- 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;
- Communication with the advisory and support services, professional associates and colleagues
- Exchange of curriculum and administrative data with LEA and DfE
- Improved access to technical support including remote management of networks and automatic system updates
- Access to learning wherever and whenever convenient.

How will Internet use provide effective learning?

- Internet access has been and will continue to be purchased from a supplier that provides a service designed specifically for pupils; this is a secure and safe site with filtering appropriate to the age of the pupils
- Internet access will be planned to enrich and extend learning activities. Access levels will be carefully monitored and reviewed to reflect the curriculum requirements and age of pupils
- Pupils will be given clear objectives for Internet use, they will be made fully aware of the need to use the search engine safely, ensuring they follow the rules from the Click clever Click Safe government initiative
- Staff will guide pupils in on-line activities that will support the learning outcomes planned for pupils' age and maturity
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be educated in taking responsibility for their own safe Internet access
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy
- Pupils will have adult supervision when accessing the Internet in school.

How will Pupils be taught to access Internet content?

Pupil e-safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - to STOP and THINK before they CLICK
    - to understand that the Internet safety rules apply to any use of the Internet regardless of which electronic device it is accessed on e.g. Play stations etc.
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be
    - to know how to narrow down or refine a search
    - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings
    - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments

- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
- to understand that some social sites have age restrictions
- to understand why they must not post pictures or videos of others without their permission
- to know not to download any files – such as music files - without permission
- to have strategies for dealing with receipt of inappropriate materials
- [for older pupils] to understand why and how some people will 'groom' young people for example-sexual reasons; radicalisation
- to understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying
- to know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP(Child Exploitation and Online Protection centre) button

- E-safety rules will be discussed with the pupils at the start of each year and revisited at appropriate times throughout the year
- Plan Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism.
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling
- Introducing the e-safety policy to pupils
- E-safety posters will be posted next to all computers within classrooms in a prominent place so that all users can see them

How will e-mail be managed?

- Staff are encouraged to use e-mail and the internet in support of their work. All use of these facilities should be appropriate to the work, standards and ethos of the school.
- The use of the school's internet and e-mail systems is not provided as a right to any of their users. They may be withdrawn from any user adult or pupil who does not conform to the schools policy.

Acceptable Use Policy

- The school is responsible for authorising any user of its internet or e-mail facilities, and should monitor and police their use
- Pupils may only use approved e-mail accounts on the school system
- Pupils must immediately tell a teacher if they receive offensive e-mail
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Where practicable, access in school to external personal e-mail accounts, including webmail accounts may be blocked
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Social Networking

- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind which may identify them or their location.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the school's preferred system for such communications.
- Staff in school should not establish or seek to establish social contact with pupils for the purpose of securing a friendship or to pursue or strengthen a relationship. This includes social networking sites such as Twitter and Facebook and blogging. Even if a pupil seeks to establish social contact, or if this occurs coincidentally, the member of staff should exercise her/his professional judgment in making a response and be aware that such social contact in person, by phone or on the internet could be misconstrued and may place the member of staff in a very vulnerable position.
- School staff will ensure that in private use:
    - No reference should be made in social media to students / pupils, parents / carers or school staff
    - 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 or local authority
    - Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Blogging

- The school will only use secure blogging sites
- Any content that is presented for the blogging site is always seen and approved by the IT technician/teacher before it is uploaded.

Managing video-conferencing

- Videoconferencing and skypeing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Videoconferencing will be appropriately supervised for all pupils' age.

What are the rules for network use?

- All staff and pupils will be required to sign an Acceptable Use Policy
- Pupils will not be allowed to access public chat rooms
- Use of the internet for inappropriate reasons will be banned for both pupils and staff
- Use polite and appropriate language at all times
- Do not use abusive language in your messages to others
- Do not reveal any information about yourself or others
- Use of the internet for inappropriate reasons will be banned for both pupils and staff
- Rules for Internet access will be posted near all computer systems
- Pupils will be informed that Internet use will be monitored
- Photographs must not identify individual pupils. Group shots or pictures taken "over the shoulder" will be used in preference to individual "passport" style images
- Full names will not be used anywhere on the Web Site, particularly alongside photographs
- Websites used will be thoroughly tested before pupils are given access to ensure the content complies fully with the borough's and school's e-safety guidelines
- A risk assessment must always be carried out before pupils are allowed to use a new technology in school
- Staff or approved adult school users should at all times abide by the copyright laws in respect of documents and materials downloaded from the internet

- Staff using a school laptop or other device off the school site, at home or elsewhere, will still have to abide by the school internet Acceptable Use Policy. Colleagues will be aware that the misuse of such devices for activity not agreed by the school may be breaking the law under the *Computer Misuse Act (1990)*

How will equipment and Digital content be managed?

- Mobile phones and other digital equipment brought into school are entirely at the staff member, students & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held digital device brought into school. All visitors are requested to keep their phones on silent.
- Mobile Phones and personally-owned digital devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned digital devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- The recording, taking and sharing of images, video and audio on any mobile phone or other digital equipment is to be avoided; except where it has been explicitly agreed otherwise by the head-teacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the head-teacher is to be able to withdraw or restrict authorisation for use at any time if it is deemed necessary.
- The School reserves the right to search the content of any mobile or handheld digital 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 digital devices may be searched at any time as part of routine monitoring.
- Mobile phones and personally-owned digital devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Staff are not permitted to use their own mobile phones or digital devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Mobile phones and personally-owned digital devices are not permitted to be used in certain areas within the school site - changing rooms and toilets.
- No images or videos should be taken on mobile phones or personally-owned mobile digital devices without the prior consent of the person or people concerned.

Students' use of personal devices

- The School strongly advises that student mobile phones or personally owned digital devices should not be brought into school.
- If a student breaches the school policy then the phone or digital device will be confiscated and will be held in a secure place in the school office. Mobile phones and digital devices will be released to parents or carers in accordance with the school policy.
- The School accepts that on rare occasions there may be exceptional circumstances in which a parent wishes their child to have a mobile phone for their own safety. This will be agreed under consultation with the head teacher and the mobile phone will be held in the school office during the school day.

Password Security

- Adult users are provided with an individual network and email login username and password.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network.

How will risks be assessed?

- Methods to identify, assess and minimise risks will be reviewed regularly
- All internet use will be monitored to ensure pupil safety. However since some material available via the Internet is unsuitable for pupils, the 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. Neither the school nor the LEA can accept liability for the material accessed or any consequences of Internet access
- The most serious risk to pupils using the internet involves the possibility of someone being hurt, exploited or abused as a result of personal information being disclosed online. Pictures, names, addresses, ages or information about a child's likes or dislikes can be used to trace, contact and meet a pupil with the intention of causing harm. The risk to children may not be immediate, since there can be a long period of building up a relationship, known as the 'grooming process'.
- Staff will be aware of the need to be vigilant for signs that children are being subjected to online sexual grooming or extremism either at home or at school. Any suspicious or evidence of such must be reported through the school's Safeguarding Procedures- to the head teacher or safe-guarding officer.

The main areas of risk for our school community can be summarised as follows:

- **Content**
  - exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse, extremist views
  - lifestyle websites, for example pro-anorexia/self-harm/suicide sites
  - hate sites
  - content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)
- The head teacher will ensure that the Internet policy is implemented and compliance with the policy monitored, delegated to the school curriculum co-ordinator.

Emerging Technologies

- Emerging technologies will be examined for educational benefit and potential risks before use in school is allowed.

School Web Site and Published Content

- The contact details on the web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Images that include pupils will be selected carefully and they will not be identified by name.
- Written permission from parents/carers is obtained before images of pupils are published electronically. This is done upon entry to school. Parents may subsequently write to agree/withdraw permission if they change their mind.

How will filtering be managed?

- The school will work in partnership with parents, the LEA, the DfES and the Internet Service Provider to ensure systems to protect pupils are up to date, regularly reviewed and as effective as possible.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- Staff will at all times work to maximise the safety of pupils within their care in their use of the internet.
- Younger pupils will not be able to use the internet unsupervised
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the IT subject leader/IT Technician and access will immediately be barred to safeguard school users
- Any material that the school believes is illegal must be referred to CEOP
- Any search engine used by pupils will be monitored carefully by staff. When getting pupils to research topics on the Internet ALL staff must check what results a keyword will bring up BEFORE allowing the children to use the search engine. Recommended search engine-www.google.co.uk
- Staff will use focused search tasks rather than very open research tasks for younger pupils to ensure that accidental access to inappropriate web sites is reduced
- Filtering strategies will be selected by the school in discussion with the filtering provider when appropriate. The filtering strategy will be selected to suit the age and curriculum requirements of the pupil

How will staff be consulted?

- All staff members: Teachers, supply staff, classroom assistants and support staff will be provided with the School Internet Policy and guidelines on e-safety and its importance explained
- All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school
- Staff development in safe and responsible Internet use, and on the school Internet policy will be provided as required
- Staff will be informed that inappropriate use of Internet resources can lead to formal disciplinary action, up to and including dismissal

How will IT system security be maintained?

- The IT subject leader/IT Technician will ensure that the system has the capacity to take increased traffic caused by Internet use
- The school IT systems will be reviewed regularly with regard to security
- Virus protection will be installed and updated regularly
- USB Media must only contain appropriate material for use in school and staff must ensure that they regularly check their media for viruses
- Files held on the school's network will be regularly checked

How will complaints regarding Internet use be handled?

- Responsibility for handling incidents will be given the Senior Management team and the head teacher
- Any complaint about staff misuse must be referred immediately to the head teacher
- Complaints of Internet misuse will be dealt with by a senior member of staff
- As with drugs issues, there may be occasions when the police must be contacted. Early contact will be made to discuss the legal position and discuss strategies
- Parents wishing to complain about an e-safety issue should use the established school complaints procedure
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy
- Complaints of a child protection nature must be dealt with in accordance with child protection procedures
- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
    - interview by relevant member of SLT
    - informing parents or carers;
    - pupil may have e-mail, Internet or computer access denied for a period of time depending on the nature of the incident.
    - Parents will be informed and will need to work in partnership with staff to resolve issues
    - referral to LEA / Police

Reporting Issues of Concern

Staff have a duty to report issues of concern e.g. sexting, extremist views (Prevent Duty) or any other safeguarding issue through the **school's Safeguarding channels**.

- Pupils will be made aware of the CEOP report abuse buttons and their use when inappropriate material is displayed (for children using sites at home).

Staff

- All staff will be given access to the School e-Safety Policy and its importance explained.
- Workshops will be held to keep staff updated on e-safety issues/developments

Parents

- Parents' attention will be drawn to the School's e-Safety Policy on the school website.
- Workshops will be held for parents to help them to become more aware of internet safety issues
- The school will support Parental responsibilities

Associated documents:

The Prevent Duty (DfE June 2015)
Keeping Children Safe in Education (DfE July 2016)