Blackmore Primary School Use of Technologies & E-Safety Policy

Date Last Reviewed	**Autumn 2018**
Ratified by the Governing Body	**Autumn 2018**
Frequency of Review	**3 Years**
Date of Next Review	**Autumn 2021**
Version	**1.0**

Introduction
This policy relates to the Safeguarding policy. The subject leader for computing will ensure that this policy is kept up to date. We believe it is essential for guidance on use of technologies in school to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote it.

New technologies are integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The resources used by pupils in school are carefully chosen by the teacher and determined by curriculum policies.

The problems and issues that have been highlighted by the media concern all schools. Whilst some of the media interest is hype, there is genuine cause for concern that children might access unsuitable material either accidentally or deliberately.

The purpose of this policy is to:

- Establish the ground rules we have in school for using technology
- Describe how these fit into the wider context of our discipline and PSHE policies
- Demonstrate the methods used to protect children from sites containing pornography, racist or politically extreme views and violence. The school 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 the school shares with parents and carers via the Acceptable Use Agreement (see appendix 1).
- Offer guidance to staff about the use of social networking sites.

Pupils' Access to the Internet
Blackmore Primary School will use the Essex County Council's filtered Internet service, which will minimize the chances of pupils encountering unsuitable material. *School* will normally only allow children to use the Internet when there is a responsible adult present to supervise. However, it is unrealistic to suppose that the teacher's attention will always be directed towards every computer screen. Member of staff will be aware of the potential for misuse and will be responsible for explaining expectations of proper use to pupils.

Teachers will have access to pupils' emails and other Internet files generated in school, and will check these periodically to ensure that expectations of behaviour are being met.

At Blackmore Primary School, we feel that the best recipe for success lies in a combination of site-filtering, of supervision, and by fostering a responsible attitude in our pupils in partnership with parents.

Using the Internet to enhance education

The benefits include:

- Access to a wide variety of educational resources including libraries, art galleries and museums;
- Rapid and cost-effective world-wide communication;
- Gaining an understanding of people and cultures around the globe;
- Staff professional development through access to new curriculum materials, expert knowledge and practice;
- Exchange of curriculum and administrative data with the Local Authority and DCSF;
- Social and leisure use;
- Greatly increased skills in Literacy, particularly in being able to research, read and appraise critically and them communicate what is important to others;
- The school intends to teach pupils about the vast information resources available on the Internet, using it as a planned part of many lessons;
- All staff will review and evaluate resources available on web sites appropriate to the age range and ability of the pupils being taught.

School Twitter
Twitter (@Blackmoreschool) will be used to share quick examples of work, events and accomplishments within the school community. Anyone may 'follow' the school Twitter page, retweet, comment on and interact with the content in a respectful manner that would be expected for any interaction that would happen on school property. Failure to comply with community standards set by Twitter and the school will result in the user being blocked form the page. The school twitter page will not be used to 'follow' any parent profiles.

Prohibited communications
Electronic media cannot be used for knowingly transmitting, retrieving, or storing any communication that is:

1. Discriminatory or harassing;
2. Derogatory to any individual or group;
3. Obscene, sexually explicit or pornographic;
4. Defamatory or threatening;
5. In violation of any license governing the use of software; or
6. Engaged in for any purpose that is illegal or contrary to the school's policy or interests.

Personal use
Computers, electronic media and services provided by the school are primarily for educational use to assist employees in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their educational purposes. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

Access to employee communications
The school reserves the right to routinely gather logs for most electronic activities or monitor employee communications directly, e.g., telephone numbers dialed, sites accessed, call length, and time at which calls are made, for the following purposes:

1. Cost analysis;
2. Resource allocation;
3. Optimum technical management of information resources; and
4. Detecting patterns of use that indicate employees are violating school policies or engaging in illegal activity.

The school reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other school policies.

Employees should not assume electronic communications are completely private. Accordingly, if they have sensitive information to transmit, they should use other means.

Under no circumstances should pupil–named data be transmitted over the Internet or email. The school office has use of encrypted data systems for this purpose.

Software
To prevent computer viruses from being transmitted through the school's computer system, unauthorized downloading of any unauthorized software is strictly prohibited. Only software registered through the school may be downloaded. Employees should use virus trapping software on any home computer that is used to download planning or other information onto the school computers. Employees should contact the headteacher if they have any questions.

Security/appropriate use
Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by school management, employees are prohibited from engaging in, or attempting to engage in:

1. Hacking or obtaining access to systems or accounts they are not authorized to use.
2. Using other people's log-ins or passwords.
3. Breaching, testing, or monitoring computer or network security measures.

No e-mail or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.

Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

Anyone obtaining electronic assess to other companies' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

Encryption
Employees can use encryption software supplied to them by the systems administrator for purposes of safeguarding sensitive or confidential business information. Employees who use encryption on files stored on a school computer must provide their supervisor with a sealed hard copy record (to be retained in a secure location) of all of the passwords and/or encryption keys necessary to access the files.

Acceptable Use Agreement: Pupils
Blackmore Primary School Computing Code of Conduct
(Acceptable Use Agreement / E-Safety Rules)

In order to keep ourselves and others safe I agree to the following:

Using computing or related technologies:

- I will only use Computing in school for school purposes.
- I will not tell other people my Computing passwords.
- I will only open/delete my own files.
- I will only access the computer system with the login and password I have been given.
- I will not access other people's files or bring in USB drives or CDs from outside school.

Using the internet:

- I will ask permission from a teacher before using the internet or sending an email.
- I will report any unpleasant material to my teacher immediately because this will help protect other pupils and myself.
- I understand that the school may check my computer files and may monitor the internet sites I visit.
- I will not complete and send forms without permission from my teacher.
- I will not give out personal information, including but not limited to my full name, my home address or telephone number.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty and if I accidentally find anything like this I will tell my teacher immediately.
- I will not enter chat rooms or leave messages on bulletin boards.
- I will ensure that my online activity, both in school and outside school, will not be inappropriate or offensive to others.
- I understand that if I deliberately break these rules, I could be stopped from using the school network and accessing the Internet.

Using e-mail:

- I will immediately report any unpleasant messages sent to me because this would help protect other pupils and myself.
- I understand that e-mail messages I receive or send may be read by others.
- The messages I send will be polite and responsible.
- I will only e-mail people I know, or my teacher has approved.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not give my personal details out, including my full name, my home address or telephone number.
- I will not use e-mail to arrange to meet someone outside school hours.
- I know that my use of Computing can be checked and that my parent/carer contacted if a member of school staff is concerned about my e-Safety.

Name …… Class …….. Date ……

Acceptable Use Agreement: Staff, Governors and Visitors
Acceptable Use Agreement / Code of Conduct

Computing (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of computing or related technologies. All staff are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher, or Deputy Headteacher.

- I will only use the school's email / Internet / Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the computing system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils/staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address and social networking identities to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without the permission of Computing Manager or technician.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of Computing and related technologies.
- This Acceptable Use Agreement is a summary of our E-safety Policy which is available on our website.

Advice to staff on the use of social networking sites

• There have been many issues with Facebook and other social networking sites in schools over the last couple of years.

• The internet is a public domain not a private one and staff in schools must be aware that information which they share and post is accessible to the public at large.

• It is therefore particularly important that staff do not name or discuss individuals – pupils, staff, parents or governors – on social networking sites. To do so would constitute a serious breach of confidentiality and data protection procedures.

• All staff in schools must also be aware that they are particularly vulnerable to accusations of inappropriate behaviour, even outside of school, and that these could potentially give rise to the involvement of the GTC and formal disciplinary procedures.

• All school staff, particularly teachers, risk exposure in the press and potential complaints to Headteachers, governors and the Local Authority when information posted on the Internet suggests behaviour which compromises their position as role models to pupils.

Our school offers the following advice to staff:

1. Ensure that you do not post any photographs on the Internet which could give cause for embarrassment.
2. Do not post any comments which could compromise your own integrity or which could bring the school, your colleagues, parents or the school community into disrepute.
3. Do not discuss school matters, including comments about pupils, staff, parents or governor on social networking sites.
4. Check that you are happy with the privacy levels on your pages and review these settings regularly.
5. You are very strongly advised **not to allow pupils to become 'friends'** on these sites. This is because it is deemed to be inappropriate to encourage out-of-school relationships with pupils and because of the nature of some of the likely content of material on sites used by adults.
6. If a complaint is received about a member of school staff then this will be dealt with under the school's disciplinary procedures and in consultation with Essex County Council's HR Schools' Team.

Access to employee communications
The school reserves the right to routinely gather logs for most electronic activities or monitor employee communications directly, e.g., telephone numbers dialled, sites accessed, call length, and time at which calls are made, for the following purposes:

1. Cost analysis;
2. Resource allocation;
3. Optimum technical management of information resources; and
4. Detecting patterns of use that indicate employees are violating school policies or engaging in illegal activity.

The school reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other school policies.

Employees should not assume electronic communications are completely private. Accordingly, if they have sensitive information to transmit, they should use other means.

Under no circumstances should pupil–named data be transmitted over the Internet or email. The school office has use of encrypted data systems for this purpose.

User Signature
I have read, understand, and agree to comply with the foregoing policies, rules, and conditions governing the use of Blackmore Primary School's computers, networks and telecommunications equipment and services. I understand that I have no expectation of privacy when I use any of the telecommunication equipment or services. I am aware that violations of this guideline on appropriate use of the e-mail, Internet systems and participation in social networking sites may subject me to disciplinary action,

including termination from employment, legal action and criminal liability. I further understand that my use of e-mail, Internet systems and participation in social networking sites may reflect on the image of Blackmore Primary School to our pupils, parents, governors and suppliers and that I have responsibility to maintain a positive representation of the school.

Signature …….. Date …….

Full Name …….. (Printed)

Role ……