Basildon C.E. Primary School
ICT Acceptable Use Policy

Document Control

Original Document:	E-safety Policy	**Date Created:**	June 2015
Version:	1.3	**Date Modified:**	May 2018
Revision due	June 2019		
Author:	Paul Field, Headteacher	**Modified by:**	Pam Slingsby, School Business Manager

Change History

Version	Date	Description	Change ID
1.0	June 2015	Initial E-safety policy	PF
1.1	July 2015	Approved by FGB	PF
1.2	December 2016	Reviewed and approved by FGB	PF
1.3	May 2018	Inclusion of Document Control and Change History Updated to reflect changes fur to GDPR Rebranded to BPS ICT Acceptable Use Policy	PSS
1.4			

Contents

1. Statement of Intent

Basildon C.E. Primary School promotes the use of technology and understands the positive effects it can have on enhancing pupils' learning and community engagement. The School recognises it must also ensure that technology is used appropriately. Any misuse of technology will not be taken lightly and will be reported to the Headteacher in order for any necessary further action to be taken.

This ICT Acceptable Use Policy is designed to outline stakeholder responsibilities when using technology, whether this is via personal devices or school devices, or on/off the school premises.

This applies to **all** staff, governors, volunteers, contractors and visitors.

Reviewed and approved by Full Governing Body on			
Headteacher		*Chair of Governors*	
Name		*Name*	
Signature		*Signature*	
Date		*Date*	

2. Introduction

2.1 This policy refers to information or data held within its systems as any item which is uniquely identifiable to a person or persons within the school community that the school has the responsibility for managing and/or protecting. This includes but is not restricted to:

- Personal details
- Medical information
- Assessment information
- Personnel information
- Digital images
- Digital recordings

2.2 This policy applies to all stakeholders (users): pupils, employees, governors, volunteers, third party staff and contractors when using school ICT facilities or information within or captured on school grounds.

2.3 The school acceptable use policy is divided into the following sections.

- General policy and code of practice
- Internet policy and code of practice
- Email policy and code of practice
- Social media policy and code of practice

2.4 This policy should be read in conjunction with the following:

- Data Protection policy
- Records Management policy
- Staff Code of Conduct

3. General Policy and Code of Practice

3.1 The school has well-developed and advanced ICT systems, which it intends all stakeholders to benefit from.

3.2 This policy sets out the rules that all must comply with to ensure that the system works effectively for everyone.

3.3 The GDPR and Data Protection Act 2018 require all personal and special category data to be processed with the utmost credibility, integrity and accuracy. This applies to all data the school stores on its network and devices regarding staff, pupils and other natural persons it deals with whilst carrying out its functions.

3.4 The school will only process data in line with its lawful basis to uphold the rights of both pupils, staff, stakeholders and other third parties.

3.5 In order to protect pupils' safety and wellbeing, and to protect the school from any third party claims or legal action against it, the school may view any data, information or material on the school's ICT systems or devices, and in certain circumstances, disclose that data, information or material to third parties, such as the police or social services. The school's Data Protection policy and associated privacy notices details the lawful basis under which the school is lawfully allowed to do so.

3.6 The school disclaimer is placed automatically at the end of emails. It notifies the recipient that any email correspondence may be monitored. It must not be removed. All stakeholders should bring to the attention of any person who wishes or intends to send an email that the school may monitor the content of their email.

3.7 Code of practice

The school's philosophy	All stakeholders or users, will follow the school's ethos and consider the work and feelings of others. Users must not use the system in a way that might cause annoyance, distress or loss of service to other users.
Times of access	The network is available during term time. Out of term time the network may be subject to maintenance downtime and may not be available for brief periods.
Nature of network	The school offers a secure network for official school activity and devices. Additionally, the school offers a 'bring your own device' (BYOD) network within limited access for general by all stakeholders.
Connections to the system	Any hardware which may be detrimental to either of the school's networks must not be used.

Ownership	All devices remain the property of the school. Such facilities are allocated on a personal basis, as required.
Copying and plagiarising	Users must not plagiarise or copy any material that does not belong to the user.
Access to information not normally available	The school's system or the internet must not be used to find facilities or flaws in the system that might give access to information or areas of the network not normally available. Users must not attempt to install software to explore or harm the system. Use of hacking tools, e.g. 'loggers', 'sniffers' or 'evidence elimination software', is expressly forbidden.
User ID and password and logging on	Users will be given unique user IDs and passwords. These must be kept private and confidential at all times. Passwords must be a mix of the following: • Contain at least six characters • A mixture of lower case and capital letters • At least one number Ideally, passwords will also contain at least special character. In the event that a password is forgotten or accidentally disclosed, it must be reported immediately to the School Network Manager. The acceptable use of any device remains the responsibility of the user logged on. Use of the school's systems are monitored and recorded remotely under the ICT support contract. Any abuse of the system will be reported to the School Network Manager. Accounts must not be shared, and permission to do this will not be granted. However, use of the school's facilities by a third party using a stakeholder's user name or password will be attributable to the stakeholder, and they will be held accountable for any misuse. Users must not log on to more than two school devices with the same user credentials.

Logging off	Users must log off from the computer they are using at the end of each of session and wait for the standard login screen to reappear before leaving. This action signals to the system that the user is no longer using the service; it ensures security and frees up resources for others to use.
Connections to the computer	Users should use the keyboard, mouse and any headphones/speakers provided. They must not adjust or alter any settings or switches without first obtaining permission from the School Network Manager. Encrypted USB memory sticks, or other portable storage media may be used where a port is provided at the front or side of a device. Users are not permitted to connect anything else to the computer without first obtaining permission from the School Network Manager.
Malware or Viruses	If a user suspects that the computer/device has a virus, or a user warning regarding malware or breach of security is displayed, the user • Must cease all activity on the device • Place a warning notice on the screen • Report the concern immediately to the School Network Manager
Installation of software, files or media	Users must not install or attempt to install software of any kind to network drives or local hard drives of networked desktop computers, without first obtaining permission from the School Network Manager. Users must not alter or re-configure software on any part of the school's system.
File space	Users must manage their own file space by deleting old data rigorously and by deleting emails that you no longer require, as defined in the associated policies. If a user believes that they have a real need for additional space, please discuss this with the School Network Manager.

Accessing, generating or saving data	Users must not access, generate or save data • On the school network • On school devices • On their personal devices whilst on school grounds that in any way contravenes the School's philosophy or associated policies and procedures, including but not limited to: • Safeguarding • Data Protection
Transferring data	Users may transfer data (e.g. files, images etc.) between school devices and networks vis • the school Google drives • encrypted removable storage media • authorised preinstalled software • authorised government platforms When transferring data, users must not import or export any material unless the owner of that material expressly permits them to do so.
Reporting faults and malfunctions	Users must report any faults or malfunctions in **writing** to the School Network Manager, including full details and all error messages, as soon as possible.
Printing	The school may check that expensive resources are being used efficiently. The School Business Manager may suggest other strategies to save on resources.
Food and drink	Users must not eat or drink when in close proximity with school devices. Users must always maintain a clean, well ordered, quiet working environment.
Copies of important work	It is the user's responsibility to keep paper copies and back-up copies, e.g. on a CD or memory stick, of their work. Any data containing personal and special category data must not be stored on unencrypted media and paper back-ups must be stored in a secure lockable location.
System backup	The school maintains a rigorous back up facility of all data held on school systems through the school's IT maintenance contract.

4. Internet Policy and Code of Practice

4.1 The school can provide access to the internet from desktop PCs via the computer network and through a variety of electronic devices connected wirelessly to the network.

4.2 Whenever accessing the internet using the school's or personal equipment you must observe the code of practice below.

4.3 This policy and code of practice is designed to reduce and control the risk of offences being committed, liabilities being incurred, pupils, staff or other stakeholders being offended and the school's facilities and information being damaged.

4.4 The School reocgnises that internet use can enhance learning:

- Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

4.4 Any breach of this policy and the code of practice will be treated extremely seriously, and it may result in disciplinary or legal action or expulsion.

4.5 The school may take steps, including legal action where appropriate, to recover from an individual any expenses or liabilities the school incurs because of the breach of this policy and code of practice.

4.6 Why is internet access available?

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for all stakeholders.

The internet is a large and very useful source of information. Numerous websites and services, both official and unofficial, provide information or links to information which would be useful for educational purposes.

4.7 Why is a code of practice necessary?

There are four main issues:

- Although the internet is often described as 'free', there is a significant cost to the school for using it. This cost includes telephone line charges, subscription costs (which may depend on how much a service is used) and the computer hardware and software needed to support internet access.

- Although there is much useful information on the internet, there is a great deal more material which is misleading or irrelevant. Using the internet effectively requires training and self-discipline. Training is available on request from ICT staff.

- Unfortunately, the internet carries a great deal of unsuitable and offensive material. It is important for legal reasons, reasons of principle, and to protect to protect the staff and pupils who access to the internet, that it is properly managed. Accessing certain websites and services, and viewing, copying or changing certain material, could amount to a criminal offence and give rise to legal liabilities.

- There is a danger of importing viruses on to the school's network, or passing viruses to a third party, via material downloaded from or received via the internet, or brought into the school on disks or other storage media.

4.8 Code of practice

Use of the internet	The Internet should not normally be used for private or leisure purposes; it is provided primarily for education or business use. Stakeholders may use the internet for other purposes provided that: • Such use is occasional and reasonable; • Such use does not interfere in any way with your duties; and • They always follow the code of practice.
Misuse, abuse and access restrictions	Users must not misuse or abuse any website or service or attempt to bypass any access controls or restrictions on any website or service.

Inappropriate material	Users must not use the internet to access any newsgroups, links, list-servers, web pages or other areas of cyberspace that could be offensive because of pornographic, indecent, racist, violent, illegal, illicit, or other inappropriate content. "Inappropriate" in this context includes material that is unsuitable for viewing by pupils. Users are responsible for rejecting any links to such material that may appear inadvertently during research. If a user encounters any material that could be regarded as offensive, they must leave that website or service immediately and not make any copy of that material. If a user encounters any difficulty in leaving a website or service, they must inform the School Network Manager immediately.
Copyright	Users should assume that all material on the internet is protected by copyright and must be treated appropriately and in accordance with the owner's rights. Users must not copy, download or plagiarise material on the internet unless the owner of the website expressly permits them to do so.
Giving out information	Users must not give any information concerning the school, its pupils or parents, or any member of staff when accessing any website or service. This prohibition covers the giving of names of any of these people – the only exception being the use of the school's name and the user's own name when accessing a service that the school subscribes to.
Personal safety	Users should take care with whom they correspond with. Users should not disclose where they are or arrange meetings with strangers they have got in contact with over the internet.
Hardware and software	Users must not make any changes to any of the school's hardware or software. This prohibition also covers changes to any of the browser settings, without first obtaining the permission of the School Network Manager. The settings put in place by the school are an important part of the school security arrangements and making any changes, however innocuous they might seem, could allow hackers and computer viruses to access or damage the school's systems.

Monitoring	The internet access system used by the school maintains a record, which identifies who uses the facilities and the use that they make of them. The information collected includes which website and services visited, how long a user remains there and which material was viewed. This information will be analysed and retained, and it may be used in disciplinary and legal proceedings.

5. Email Policy and Code of Practice

5.1 The school's computer system enables members of the school to communicate by email with any individual or organisation with email facilities throughout the world.

5.2 For the reason outlined above, it is essential that a written policy and code of practice exists, which sets out the rules and principles for use of email by all.

5.3 The email sent, received and stored within the school's email system remains the property of the school. Users are required to manage the information therein in accordance with the School's Data Protection and Record Management policies.

5.4 Any breach of this policy and code of practice will be treated seriously and it may result in disciplinary or legal action or expulsion.

5.5 The school may take steps, including legal action where appropriate, to recover from an individual any expenses or liabilities the school incurs because of the breach of this policy and code of practice.

5.6 Code of practice

Purpose	Users should only use the school's email system for work related emails. Users are only permitted to send a reasonable number of emails.
School disclaimer	The school's email disclaimer is automatically attached to all outgoing emails and this must not be removed, cancelled or disapplied.

Security	As with anything else sent over the internet, emails are not completely secure. There is no proof of receipt, emails can be 'lost', they can suffer from computer failure and a determined 'hacker' could intercept, read and possibly alter the contents. As with other methods of written communication, the user must make a judgment about the potential damage if the communication is lost or intercepted. Every effort should be made **not** to send confidential information, including personal information or passwords, by email.
Quality	Emails constitute records of the school and are subject to the same rules, care and checks as other written communications sent by the school. Emails will be checked under the same scrutiny as other written communications. **All users** should consider the following when sending emails: • Whether it is appropriate for material to be sent to third parties • The emails sent and received may have to be disclosed in legal proceedings • The emails sent and received maybe have to be disclosed as part of fulfilling a Subject Access Request • Whether any authorisation is required before sending • Printed copies of emails should be retained in the same way as other correspondence, e.g. letter • The confidentiality between sender and recipient • Transmitting the work of other people, without their permission, may infringe copyright laws. • The sending and storing messages or attachments containing statements that could be construed as abusive, libelous, harassment may result in disciplinary or legal action being taken. • Sending or storing messages or attachments containing statements which could be construed as improper, abusive, harassing the recipient, libelous, malicious, threatening or contravening discrimination legislation or detrimental to the is a disciplinary offence and may also be a legal offence.

Confidential Emails	You must ensure that confidential emails are always suitably protected. If working at home or remotely, users should be aware of the potential for an unauthorised third party to be privy to the content of the email. Confidential emails must be deleted when no longer required.
Inappropriate emails or attachments	Users must not use email to access or send offensive material, chain messages or list-servers or for the purposes of bullying or plagiarising work. Users must not send personal or inappropriate information by email about themselves, other members of staff, pupils or other members of the school community. If users receive any inappropriate emails or attachments, they must report them to School Network Manager immediately.
Program files and non-business documents	Users must not introduce program files or non-business documents from external sources on to the school's network. This might happen by opening an email attachment or by downloading a file from a website. Although virus detection software is installed, it can never be guaranteed 100 percent successful, therefore introducing nonessential software is an unacceptable risk for the school. If users have any reason for suspecting that a virus may have entered the school's system, you must contact the School Network Manager immediately.
Viruses	If users suspect that an email has a virus attached to it, they must inform the School Network Manager immediately.
Spam	Users must not send spam (sending the same message to multiple email addresses) where not applicable to school business, without the permission of Headteacher.
Storage	Old emails may be deleted from the school's backup after 12 months. Users are advised to regularly delete material they no longer require and to archive material required to be kept. For further information please see our Records Management Policy.

Message size	Staff are limited to sending messages with attachments which are up to 5Mb in size. Larger files should be distributed within the school by using shared network areas.
Monitoring	Copies of all incoming and outgoing emails, together with details of their duration and destinations are stored offsite (in electronic form). The frequency and content of incoming and outgoing external emails are checked termly to determine whether the email system is being used in accordance with this policy and code of practice. The Headteacher and School Network Manager are entitled to have read-only access to user emails.

6. Email Policy – Advice

Owners of school provided email accounts should remind themselves of the ICT Acceptable Use Policy which relates to the monitoring, security and quality of emails. In addition, such account owners should be guided by the following good practice:

- Check emails daily and respond, as appropriate, within a reasonable period if the email is directly addressed to them.
- Avoid spam, as outlined in this policy.
- Avoid using the email system as a message board and thus avoid sending trivial global messages.
- Whilst accepting the convenience of the distribution lists, users should try to restrict their use to important or urgent matters.
- Emails should be sent to the minimum number of recipients.
- Emails should always include a subject line.
- Old emails are kept for the minimum time necessary.

7. Social Media Policy and Code of Practice

7.1 The School may use social media to promote itself in the marketplace.

7.2 The School will restrict the access to social media sites for pupils.

7.3 With internet safety in mind, the School will advise pupils

- Not to access social media sites

- Of age restrictions for accessing social media sites
- Not to post personal photos on social media sites and will discuss the future implications of doing so
- Of the potential risks of accessing social media sites such as Facebook, Snapchat, Instagram etc.
- Of the potential risks of online social gaming and chatroom activities.

7.4 Any breach of this policy and code of practice will be treated seriously and it may result in disciplinary or legal action or expulsion.

7.5 The school may take steps, including legal action where appropriate, to recover from an individual any expenses or liabilities the school incurs because of the breach of this policy and code of practice.

7.6 Code of practice

Use of Social Media sites	The Headteacher will authorise designated staff to promote the school and its activities on social media sites for marketing purposes.
Access to Social Media sites at school	Access to such sites via the school internet provision is restricted to staff user logon credentials.
Communication	The school uses a variety of methods to communicate to parents/carers and other stakeholders: • the website • newsletters • letters • verbal discussion On occasion, the school may consider it appropriate to post an urgent message or update via its social media presence. School policies and documents provide further information regarding appropriate channels of communication and means of resolving differences of opinion. Effective communication following principles of mutual respect is vital for the school's reputation, especially via social networking.
E-safety	Pupils and staff will be advised how to staff safe online regularly. This topic is covered in depth across the academic year and has a particular focus during PSED week.

Monitoring	All users are to be aware that the access to such sites is monitored. The information collected includes which website and services visited, how long a user remains there and which material was viewed. This information will be analysed and retained, and it may be used in disciplinary and legal proceedings.
Staff and Governors: Personal use of social media sites	Staff and governors are reminded that • Discretion and professional conduct is essential. • Social media sites must not be accessed during lesson or work time for their personal use. • Social networking should only be used in a way that does not conflict with the current National Teacher's Standards. • All should read and comply with 'Guidance for Safer Working Practice for Adults who Work with Children and Young People'. • Pupils must **never** added as 'friends' onto their personal social media accounts (including past pupils under the age of 16). • It is **strongly advised** that personal accounts name are adjusted to protect staff and governors being stalked or targeted by other members of the school community. • It is **strongly advised** that staff and governors do not identify their school on social networking sites as this could directly link their behaviour outside of work with the reputation of the school. • Comments **must not** be posted about the school, pupils, parents or colleagues including members of the Governing Body. • Privacy settings **must be** reviewed and adjusted to give them the appropriate level of privacy and confidentiality. • Inappropriate use by staff should be referred to the Headteacher in the first instance and may lead to disciplinary action. • The use of the school's name, logo, or any other published material should not be used without written prior permission from the Headteacher.

Parents/carers and the wider school community: Personal use of social media sites	Parents and carers will be made aware of their responsibilities regarding their use of social networking. Parents **must not** post pictures of pupils, other than their own children, on social networking sites where these photographs have been taken at a school event. Parents should make complaints through official school channels rather than posting them on social networking sites. Parents **should not** post malicious or fictitious comments on social networking sites about any member of the school community.
Inappropriate Use of Social Media	In the case of inappropriate use of social media by staff, the Headteacher will direct the staff member to remove such comments or material. In the case of inappropriate use of social media by parents and the wider school community, the Governing Body will contact the individual asking them to remove the comments and seek redress through the appropriate channels such as the Complaints Policy and will send a formal response by letter.

8. Further guidelines

- Remember – emails remain a written record and can be forwarded to others or printed for formal use.
- As a rule of thumb, users should be well advised to only write what they would say face to face and should avoid the temptation to respond to an incident or message by email in an uncharacteristic and potentially aggressive fashion.
- Remember, “tone” can be misinterpreted on the printed page and once it is sent it could end up in the public domain forever. Email and social media posts lack the other cues and clues that convey the sense in which what is said should be taken, and can easily convey the wrong impression.
- Remember that sending emails from a school account is similar to sending a letter on school letterhead; **do not** say anything that might bring discredit or embarrassment to yourself or the school.
- Given the popularity and simplicity for recording both visual and audio material, all users are advised to remember the possibility of being recorded in all that they say or do.