ICT Acceptable Use & Information Security Policy

Drafted: September 2017
Ratified by the Headteacher & Personnel Portfolio Governor: September 2017
Review Date: September 2020

1. Introduction

This document defines the acceptable use of ICT equipment and services for staff at West Blatchington Primary & Nursery School and is mandatory for all staff and governors.

The availability of complete and accurate information is key to providing excellent services to the pupils, parents and staff of West Blatchington Primary & Nursery School. A large amount of sensitive and personal information on individuals, both pupils and staff, is held by the school.

The school has a number of responsibilities to protect its reputation as well as safeguarding individuals from the possibility of information and systems misuse or infringement of personal privacy. Therefore the confidentiality, integrity and accountability of this information need to be protected from harm in a way that is proportionate to the risks to the information.

This information security policy provides the overall framework to help everyone play his or her part in protecting pupil and staff information.

2. Scope

This policy applies to all users accessing any ICT systems (such as computers, hand held devices, or any information storing or processing devices) and information owned and/or operated by West Blatchington Primary & Nursery School. Its application extends to the use of all such equipment wherever situated.

This policy applies to everyone who reads or processes school information and applies wherever and whenever school information is processed. It applies equally to all users including:

- Teachers, Governors, Teaching Assistants, Support staff and office staff
- Contractors, consultants, casual and temporary employees and volunteers
- Partner and suppliers

Please note that throughout this document, the words “staff”, “employee” and “user” are used to cover all the groups of people listed above.

The information security policy applies to all forms of information, including, but not restricted to, text,

pictures, photographs, maps, diagrams, video, audio, CCTV and music, which is owned, administered or controlled by the school, including information which is:

- Spoken
- Written on paper or printed out from a computer system. This may include working both on site or remotely (e.g. at home)
- Stored on the school server, school provided Office 365 platform and the cloud
- Stored in manual filing systems
- Transmitted by electronic mail, fax, over the internet and via WiFi technology
- Stored and processed via computers, networks or mobile computing devices, including but not restricted to PCs, mobile phones, laptops, tablets and iPADs
- Stored on any type or removable computer media including, but not restricted to, CDs, DVDs, USB memory sticks, external hard disks, and memory stores in devices such as digital cameras and MP3 and MP4 players.

3. Purpose

The purpose of this information security policy is:

- To protect the school's information and subsequently to protect the school's reputation
- To enable secure information sharing to deliver services
- To protect the school from legal liability and inappropriate use
- To encourage consistent and professional use of information and systems
- To ensure everyone is clear about their roles in using and protecting information
- To maintain awareness of information security
- To protect school's employees
- NOT to constrain reasonable use of information in support of normal business activities of the school

This policy shall be seen as additional to all other school policies relating to information disclosure and personal conduct.

4. Personal and Sensitive Information

Personal information is:

- Defined as any combination of data items that identifies an individual and provides specific information about them, their achievements and their families
- That could include: names, contact details, gender, dates of birth, unique pupil number etc.
- It could also include: academic achievements, skills and abilities, progress, behaviour and attendance

Sensitive data is specifically defined as information relating to:

- A person's racial or ethnic origin
- Political opinions
- Religion or beliefs
- Membership of a trade union
- Physical or mental health
- Sexual life
- Alleged offence or any proceedings for any offence

By its nature this information needs to be treated with greater care than other personal data.

5. Managing Information Systems

5.1 Information System Security

- The Headteacher is the Senior Information Risk Owner (SIRO).
- Information shall be used legally at all times, complying with UK and European law. All users, including employees and agents of the school might be held personally responsible for any breach of the law.
- All personal information processed electronically or held in a structured manual filing system shall be processed in accordance with the Data Protection Act. Utmost care shall be taken when dealing with personal and sensitive information to ensure that it is never disclosed to anyone inside or outside the school without proper authorisation.
- Personal, confidential or sensitive information shall be protected appropriately at all times and in particular when removed from school premises either physically on paper or electronic storage devices, when transmitted electronically outside the school or within areas of the school in which the public may be present.
- Information, including text, still and moving pictures, photographs, maps, diagrams, music and sound recording shall not be saved, processed or used in breach of copyright.
- The school shall only use licensed software on its computers, servers and other computing devices.
- The schools server will be backed up to an offsite location each night.
- Security strategies will be discussed with the school's ICT contractor and ICT Schools and Traded Services Team.
- Anti-virus protection will be updated regularly. Staff with school laptops will have anti-virus protection installed by the ICT technician which will update at home if it is connected to the internet. If not connected to the internet, then staff will need to log on to their laptop at school to update on a regular basis.
- The security of individual staff and pupil accounts will be reviewed regularly. Both staff and pupils must be informed of the importance of not sharing passwords.

- The administrator account password will be changed if it becomes known.
- Computers and mobile devices may not be connected to the school network, both physically or wirelessly, without specific permission from the Business Manager/Headteacher/ICT Coordinator. Nor shall any personally owned or non-school equipment be connected to the school computer network or to any school owned equipment, whether on the school's network or not, without written permission from the Business Manager/Headteacher/ICT Coordinator.
- Portable media may not be used without specific permission from the Business Manager/Headteacher/ICT Coordinator.
- Unapproved system utilities and executable files will not be allowed to be installed or attached to emails.
- No software will be installed on or removed from West Blatchington Primary & Nursery School equipment without permission from the ICT co-ordinator/technician.
- Users shall not interfere with the configuration of any computing device without approval.
- Staff have secure areas on the network to store work related personal or sensitive files. No personal documents i.e. from home, should be stored on the school network or equipment.
- Details of school owned hardware will be recorded in a hardware inventory.
- School equipment, facilities and information shall be used only for school's business purposes, unless written permission of the Headteacher has been obtained. School equipment, facilities and information must never be used for personal gain or profit nor for electronic harassment of any kind or any action which may be to the detriment of West Blatchington Primary & Nursery School.
- School equipment, facilities and information shall be not used for private or personal interests or business, where such use is deemed to be excessive or unreasonable, especially in the use of Internet or electronic mail services. Nor shall resources be wasted (e.g. people, capacity, computer).
- Files will not be removed from a shared area without specific permission, unless the retention period for the document has expired
- The Business Manager and ICT technician will review system capacity regularly.
- Only West Blatchington Primary & Nursery School employees or authorised 3rd parties can connect to the school networks.
- Temporary guest accounts must be used for short term visitors for temporary access to appropriate systems e.g. supply accounts.
- Staff must use appropriate remote access facilities where provided.
- Employees must not install or use any encryption software other than that provided by the school.
- Staff must not log onto the school's network using someone else's user credentials (id), name and password.
- Personal data must not be stored on school servers without specific permission from the Head Teacher or ICT Coordinator
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held the school will hold a certificate of secure deletion for any server or PC that once contained personal data.

- Staff must Log Off if they are leaving the computer / room for a longer period, so that other staff can log in and access the network if they need to. If a number of staff are logged into a single machine it will slow down significantly.
- When staff leave the PC temporarily they must ensure that they lock it so that no-one can access their log in and associated networks and files.
- Unacceptable use of the school network may include, but not be restricted to:
  - Wasting of resources (e.g. people, capacity, and computer).
  - Alteration or destruction of the integrity of computer-based information.
  - Compromising the privacy of users or confidentiality of data.

5.2 Email

- Only school provided email accounts may be used for school business.
- Emails sent to external organisations that are work related must be sent from a school email address.
- Staff must not let anyone else use their account nor share their password, in school or at home.
- Personal, confidential and sensitive information sent to recipients external to the school must be encrypted using Egress encryption.
- The forwarding of chain letters is not permitted.
- Access in school to external personal email accounts may be blocked.
- Staff must use their LA email (Office 365)/school account for all emails relating to school matters. Staff personal e-mail addresses should not be accessed by pupils or parents. Any e-mail sent between staff and parents/carers should be sent through their school account and the Head Teacher should be copied in.
- If staff wish to access their school email on their own personal mobile device a consent form must be completed and submitted to the ICT Schools and Traded Services Team. These forms are available at the school office.
- Email addresses should be published carefully, to avoid email harvesting for spam purposes.

5.3 Passwords

- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private. Passwords must always be kept private and not shared with anyone under any circumstances, including with supply staff.
- If a password is compromised the school should be notified immediately and the password changed.
- Strong passwords must be used on the school network i.e. it must contain lower case and upper case letters, numbers and special characters
- Staff are required to change their network password every 60 days/every term.
- Users shall not attempt to access information to which they do not have authority.
- Staff using critical systems, such as CPOMS, must use two factor authentication.
- The Office will give details of the restricted Supply log-in and password to any supply teachers.

5.4 Use of the Internet and E-Safety

- Refer to the school's E-Safety policy for information on the use of the Internet and E-Safety.
- Staff members must not give their personal contact details including details of any blogs or personal social media sites or other websites to pupils or former pupils (see also Social Networking Policy).
- Staff members must not have contact through any personal social medium with any pupil, whether from this or any other school, unless the pupil is a family member or it is through school approved sites as part of official collaborative work (see also Social Networking Policy).
- While staff will often take photographs of children as evidence of work or to record or celebrate an event it is crucial they follow the guidelines set out in the school's E-Safety policy. These guidelines also pertain to any film made of children whether for intervention work e.g. Video Interactive Guidance, Film Club or indeed any other filming of any kind.

5.5 Printing

Staff must:

- When printing personal or confidential material, ensure that a secure printing method is used.
- Not leave personal or sensitive information on the printer, it must be collected from the printer as soon as it is printed and either password protected or sent to a secure print queue
- Not send children to collect documents from the printer, children are not permitted in the PPA room.
- Ensure that all pupil and parent information printed for a school trip or off site event is shredded after use.

5.6 Use of WiFi, iPads and Tablets, Mobile Phones, Cameras and Mobile Devices

- Staff use of mobile phones for personal reasons is strictly restricted to non-teaching times and in the staff room or a private office only. Mobile phones should be kept on silent or turned off.
- Mobile devices brought into school are entirely at the owner's risk. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices. Phones should not be carried on the person e.g. in pockets and should be stored away securely.
- Some staff with particular family circumstances may feel the need to have their mobile with them at all times in case they need to be contacted with regards to a family member. This must be approved in advance by their line manager. In this case mobiles must be on silent and no staff member should make any calls or send texts during class / teaching time unless it is an emergency. If this is the case the staff member should ask another adult to take over and leave the room while they do so.
- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children or their families within or outside of the school.
- Mobile phones or any personal cameras/iPads/tablets must not be used to take or store images of children – only school cameras and iPads can be used for this.
- Files on school cameras must not be downloaded onto devices not owned by the school.
- Cameras must be locked away, at school, at the end of each day, unless being used on a residential trip.

- Images may only be stored on school based devices and not on devices kept at home.
- Unless parent/carer permission is sought, images may only be used in school displays or records.
- Parents are confirm whether they consent to the publication of their children's photos in school publications, the prospectus, school website and media publications. Please see the school's Parental Consent Form for further details. Parental consent for any other or exceptional publication would be sought on a case by case basis.
- The use of images on the school website must be monitored by the Business Manager and Headteacher, and must be permitted by parents/carers. Unless absolutely necessary, names should not be attached. For a news item on the newsletter or website, when a name may be required only the first name of a pupil should be used (no surname).
- Any use of webcams should be strictly monitored and only be used in planned and approved curriculum enhancement opportunities.
- The use of all images of pupils must be closely monitored by the Head Teacher and ICT co-ordinator.

5.7 Working From Home

Staff must:

- Use only an encrypted device to transport personal and sensitive information out of school. Any USB stick used for personal or sensitive school information must be a school provided encrypted stick.
- Ensure that any school laptop taken home is encrypted, unless only remote access is used and no school information is stored on the hard drive.
- Always store paper and electronic information securely when away from school.
- Ensure that family members and other persons not employed by West Blatchington Primary & Nursery School do not have access to any school data.
- Not store personal or sensitive information or school owned mobile devices in the car.
- Not allow others to use school laptops or USB sticks under any circumstances.

5.8 Paper Information and Storage

Staff must:

- Ensure that all paper containing personal or sensitive information is stored securely at all times, especially in the office, and classrooms after school hours and when working from home.
- Ensure that no personal or sensitive information is displayed on classroom walls or in areas where it can be seen by the public.

5.9 Use of PCs in Classrooms

Staff must:

- Lock the screen of a PC (using Windows+L or Ctrl+Alt+Del) when leaving the PC unattended, at all times.
- Not allow anyone else to use a PC that they are logged in on.

- Not leave children unattended in the classroom using their PC

5.10 Use of USB Sticks, Removable Memory Devices and Laptops

- Only school owned, encrypted memory sticks ('4GB Data Traveler vault privacy 3.0' or '16GB Data Traveler Locker+G3') may be used at school and only these devices can be used to store personal and sensitive information. These must not be backed up at home. They should be backed up on individual drives on the shared network.
- Removable memory devices should not be used on the school network.
- If any school owned devices (memory sticks, cameras tablets etc.) are lost or stolen it must be reported immediately to a member of the SLT.
- Adequate protection must be given to any device holding sensitive or personal data to prevent unauthorised access.
- School laptops will be encrypted if they contain personal or sensitive information.
- Tablets and laptops **which have been encrypted** may be taken home and **used for work purposes only**. If they are lost or stolen it must be reported to SLT immediately.

5.11 Use of Website and Storage of Data in the 'Cloud'

- The school website shall only be used to promote the school, the education of our pupils and communication with parents/carers and the wider community. All content is strictly controlled and monitored by the Business Manager and Head Teacher.
- The school website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- No personal or sensitive information may be stored in the cloud unless a suitable level of security, which includes two factor authentication, is used, and conforms to DfE guidance. Dropbox does not provide suitable security measures for personal or sensitive information and therefore must not be used to store such data.

5.12 Retention of Data and Data Disposal

- Information must be stored in accordance with the Data Protection Act 1998 and Freedom of Information Act 2000 and must not be stored for any longer than stated in the retention schedule.
- The school uses the Information Records Management Society Toolkit for Schools V5 as the retention schedule and information shall be disposed of in accordance with this policy. The retention schedule refers to all information, regardless of the media in which it is stored.

5.12 Review of the Information Security Policy

This document shall be reviewed on a regular basis and at least annually. This policy and any associated policies shall be updated according to:

- Internally generated changes such as changes in service strategy, organisations, locations and technology.
- Externally generated changes such as changes in legislation, security threats, security incidents,

recommended best practice and audit reports.

- All changes shall be approved by the Head Teacher and the Governing Body and be made available to everyone to whom it applies.

6. Breaches of Information Security

- Actions or neglect leading to a breach of this policy will be investigated, which could result in disciplinary action; this could include dismissal without notice even for a first offence if sufficiently serious.
- Any actual or suspected breaches of any security policy within, or affecting, West Blatchington Primary & Nursery School's systems will be thoroughly investigated by the Head Teacher and other relevant staff. If staff are involved, disciplinary action (following current agreed disciplinary procedures) may be taken. Any action taken internally does not preclude prosecution through a court of law.
- Breaches of this policy by a user who is not a direct employee of the school may result in action being taken against the user and/or their employer.
- In certain circumstances the matter will be referred to the police to consider whether criminal proceedings should be instigated.
- Breaches of the Data Protection Act 1998 could result in a large fine being issued to or criminal proceedings taken against the individual or the school.
- Should a member of staff believe that this policy or aspects of the Data Protection Act 1998 have been breached, they should report it immediately to the Headteacher.

7.1 Use of the ICT technician's time:

- Staff may not use the working time of the ICT technician to support them with any ICT advice or support which is not directly linked to school business. They will not be available to mend or maintain any devices not used by the school. If damage or maintenance to any school equipment is required due to non-school business the person responsible for that damage will liable for any costs incurred in delivering the required repairs or maintenance.
- The time of the ICT technician will be managed and directed by the Business Manager.
- Requests for ICT support can be made through emailing support@focusit.freshdesk.com or for urgent issues such as the failure of network drives or a security breach, please also call Focus IT on 0330 0242001. The ICT technician will prioritise requests based on school priorities.
- For any issues regarding the internet connection please call Schools ICT on 01273 293663.

8.1 Responsibilities for saving energy and resources:

All staff must take responsibility for saving energy and resources with regards to ICT. This includes:

- Turning off data projectors at lunchtimes and after school.
- Turning off all devices at the end of the day.
- Monitoring pupil activity appropriately to ensure resources are not wasted.

9. Compliance

This policy has been issued with the authority of the Head Teacher and governors and compliance with its principles is mandatory for all employees of West Blatchington Primary & Nursery School and authorised third party users accessing any computer system owned or operated by the school.

10. Definition

All references in this document to the 'school' shall be deemed to refer to West Blatchington Primary & Nursery School.

11. Interpretation

In the event of an issue arising from an interpretation of this policy, it should be resolved by reference to the Head Teacher and ICT co-ordinator.

12. Reference Documents:

E-Safety Policy

Social Networking policy

Computing Policy

Data Protection Guidelines

Safeguarding Policy

Parental Consent Form

Appendix 1 – Copy of the Staff ICT Policies Agreement Form

Staff ICT Policies Agreement

Covering ICT Acceptable Usage Policy, E-Safety Policy and Social Networking Policy

E-Safety Policy & Social Networking Policy

Summary of Key Guidelines:

- The school owns the computer network and can set rules for its use.
- It is an offence to use a computer or network for a purpose not permitted by the school.
- Network access **must** be made via the user's authorised account and password, which must not be given to any other person (i.e. colleagues or supply teachers)
- You **must** remember to log off your computer and email account to ensure child protection whenever you are not at your PC.
- All network and internet use **must** be appropriate to education within school working hours.
- Copyright **must** be respected (images used must be copyright free).
- Messages shall be written carefully and politely particularly as emails could be forwarded to unintended readers.
- Anonymous messages and chain letters are **not** permitted.
- Do **not** browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Use of websites for personal financial gain, gambling, political activity, advertising or illegal purposes is **not** permitted (however, viewing a trade union site is permitted).
- Staff must not use the school wifi for their own mobile devices including smart watches.
- **Do not** give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents or carers. Always provide outside agencies with the school contact details and your school email address.
- The use of mobile phones is **not** permitted in the presence of children. Photographs and videos of children **must not** be taken on mobile phones (see Safeguarding Policy).
- School mobile phones should be used during residential trips and day visits. Personal mobile phones should **not** be used to contact parents. There is a school mobile phone on each site.
- Personal cameras (including those on mobile devices) **must not** be used in school or during out of school hours events. Always use school cameras for photographing children and **do not** store photographs on your school laptop or memory sticks.
- After school trips and off site events, all pupil information (including parent contact information) must be shredded after the trip.
- Ensure that your online activity, **both in school and outside school**, will not bring your organisation or professional role into disrepute.
- Do **not** state that you work at West Blatchington Primary & Nursery School on any personal social media site

or online profile, to ensure that any personal opinions do not reflect upon or link to the school.

You have a duty to report any E-Safety incident which may impact on you, your professionalism or your organisation.

The use of social networking sites is permitted **but** staff are reminded to use them in a **professional manner** and according to the guidance set out in the ICT Acceptable Usage Policy, E-Safety Policy and Social Networking Policy.

I hereby agree to the above rules. I also confirm that I have read and will adhere to both the E-Safety & Social Networking Policies and that it is my responsibility to keep up to date with the school's most recent policies.

Signed: _____ **Date**: _____

ICT Acceptable Use & Information Security Policy

I have read and understood West Blatchington Primary & Nursery School's ICT Acceptable Use & Information Security Policy and agree to abide by all the points above in this document and its guidelines and recommendations during my time of employment at West Blatchington Primary & Nursery School.

I understand that all school information that I have access to during my employment remains the property of the school following the termination of my employment at the school. I agree not to divulge any information inappropriately according to this policy following the termination of my employment at the school.

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

I understand that failure to comply with this agreement could lead to disciplinary action.

Signed: _____ **Date**: _____

Print Full Name: _____

Job Role: _____

Appendix 2 – ICT Acceptable Use Agreement for EYFS & KS1 Pupils

ICT Acceptable Use Agreement for EYFS and KS1 pupils

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I will only use usernames and passwords that are given to me
- I know that if I break the rules I might not be allowed to use a computer / tablet

Name:

Class:

Signed (child):

Appendix 3 – ICT Acceptable Use Agreement for KS2 Pupils

ICT Acceptable Use Agreement for KS2 pupils

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that West Blatchington Primary School will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger" when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc).
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for file sharing or video broadcasting (eg YouTube).

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *school*:

- Personal devices (mobile phones) should not be used in school (including school events such as school discos) and has to be stored in the school office during school times if needed. My parents/carers must complete a consent form and hand it into the school office if they want me to bring my mobile into school.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not try to access social media sites at school.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I understand that I am responsible for my actions, both in and out of school:
- I understand that the school will follow up incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, there will be consequences to my actions e.g. loss of access to the school network / internet, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement.

- I have read and understand the above and agree to follow these guidelines when:
- I use the school *s*ystems and devices
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email e.g. PurpleMash etc.

Pupil Name: .....

Class: .....

Signed: .....

Date: .....