Bellevue Place
EDUCATION TRUST

Rivermead Primary School

Acceptable use of ICT Policy

Signed:	
Chair of Trust Board:	Claire Delaney
Approved:	1 September 2022
Renewal:	2 Years
Review Date:	September 2024

Contents

1. Bellevue Place Education Trust – Our commitment 3
2. Introduction 3
3. General Statement on Acceptable Use - Staff 5
4. File storage 5
5. Internet services 7
6. E-Security 10
7. Using social media 13
8. Accessing school or BPET data off premises 13
9. Care of equipment 13
10. Data Protection 13
11. Computer security 14
12. Transferring data away from computer systems 15
13. Mobile devices 15
14. Reporting and Consequences of Non-Compliance 16
15. Policy Status 16
16. Related Policies 16
17. Monitoring and review 16

1. Bellevue Place Education Trust – Our commitment

Learn. Enjoy. Succeed.

Every BPET child and staff member enjoys a broad (LEARN) and enriched (ENJOY) learning experience, enabling them to achieve far greater individual success (SUCCEED) than they might previously have thought possible.

Our Mission

To grow hubs of like-minded, autonomous schools with a strong support network, all of which combine academic rigour with highly enriched opportunities that deliver a personalised approach to education and exceptional outcomes for all.

Our Difference

We are leading the way in delivering high quality education through skills-based and knowledge rich curricula, applying the best of the independent and state sectors to deliver breadth of opportunity and pupil enrichment. We empower all our schools as individual entities that best meet the needs of the communities they serve and have a strong relationship with families, who are our key partners in delivering the vision.

Our Promise

Every child is an individual. Our role is to nurture pupils' potential through a personalised approach to learning. BPET children are happy, independent, confident all-rounders. Our focus is ensuring an exceptional provision for all our children with supportive, accessible learning that enables every child to make progress, including high quality inclusion for children with Special Educational Needs. We encourage a 'be interested and be interesting' attitude in children and staff alike. We don't just teach; we want our pupils to have a passion to learn.

2. Introduction

- This Policy provides the guidelines of acceptable use of Information Communications Technology (ICT) equipment and facilities within Bellevue Place Education Trust (BPET).

- ICT is seen as beneficial to all members of BPET in supporting learning, teaching, research, administration and approved business activities of the Trust. The school's ICT Facilities provide a number of integral services and, therefore, any attempt to misuse a computer system could cause significant disruption to other users in BPET. This could also lead to a breach of the data protection rights of individuals, resulting in harm to that individual and BPET.

- BPET assumes the honesty and integrity of its ICT users including staff and contracted personnel/ consultants. The purpose of the Acceptable Use Policy is not to impose restrictions that are contrary to established culture of openness, trust and integrity within BPET. This policy is designed to protect all authorised users from illegal or damaging actions by individuals, either knowingly or unknowingly.

- Facilities are provided for business use only. BPET may review any activity and analyse usage patterns for the maintenance of business productivity and continuity.

- BPET is bound in this regard by the provisions of the Data Protection Act 2018 (UK GDPR), European Human Rights legislation, the Privacy and Electronic Communications (EC Directive) Regulations 2003, and the Regulation of Investigatory Powers Act 2000.

Policy Scope

- This policy applies to staff, contractors, Trustees, Members and local advisers within BPET.
- It is the responsibility of all individuals in BPET to familiarize themselves with this policy and comply with its provisions.

- The Headteacher is responsible for ensuring the safety, including e-safety of members of the school community. The day-to-day responsibility for e-safety may be delegated to the ICT Subject Leader or another appropriate member of staff. However, the Headteacher will ensure: Staff with e-safety responsibilities receive suitable and regular training enabling them to carry out their e-safety roles and to train other colleagues as necessary. The Senior Leadership Team (SLT) receives regular monitoring reports. There is a clear procedure to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The ICT Technician/Network Manager and, where appropriate, the Learning Platform Lead, will, in co-operation with the school's technical support provider, be responsible for ensuring that all reasonable measures have been taken to protect the school's network(s), ensure the appropriate and secure use of school equipment and protect school data and personal information. This will involve: Ensure the ICT infrastructure is secure and protected from misuse or malicious attack; The school meets the e-safety technical requirements outlined in any relevant academy e-safety policy/guidance; Users may only access the school's network(s) through a properly enforced password protection policy, in which passwords are regularly changed; The school's filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person ; E-safety technical information is kept up to date, applied as necessary and passed on to others where relevant; Use of the network, learning platform and pupil IT usage are regularly monitored and any misuse/attempted misuse reported to the headteacher and IT Technician for investigation and action; Appropriate steps are taken to protect personal information and secure data on all devices and removable media; Provide secure access to the school network from home where necessary using VPN or equivalent technologies.
- Teaching and support staff are responsible for ensuring that: They are familiar with current e-safety matters and the schools Acceptable Use of ICT Policy and practices; They have read and understood the school's Staff Acceptable Use Policy (AUP) and signed to indicate agreement; They report any suspected misuse or problem to the headteacher and IT Technician for investigation and action; Digital communications with pupils (e-mail/learning platform/voice) should be on a professional level and only carried out using approved school systems; E-safety issues are embedded in all aspects of the curriculum and other school activities so that pupils understand and follow the school's Acceptable use of ICT Policy; They have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations in relation to their age; They monitor ICT activity in lessons, extra-curricular and extended school activities; They are aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement school policies with regard to these devices; In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and there is awareness of the procedure for dealing with any unsuitable material that is found in internet searches.

Definitions

- BPET means all school within Bellevue Place Education Trust, as well as the central team.
- Executive Leadership Team means the Chief Executive Officer ("CEO") and the direct line management reports of the CEO (the "Directors").
- ICT Facilities means all IT devices, facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, personal organisers, music players, software, websites, web applications or services and any device, system or service which may become available in the future which is provided as part of the ICT service.
- Users means directors, members, trustees, local advisers, staff, students, trainees, volunteers, temporary guests, and all other persons authorised by BPET to use the ICT Facilities.
- Personal use means any use or activity not directly related to the users' employment, study or
- purpose.
- Materials means files and data created using the ICT Facilities including but not limited to documents, photographs, audio, video, printed output, web pages, social networking sites, bulletin boards, newsgroups forums and blogs.

3. General Statement on Acceptable Use - Staff

- The user agrees not to upload, download, post, email or otherwise transmit or store anything that:
  - ✓ is unlawful, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libellous, invasive of anyone's privacy, hateful or racially, ethically or otherwise objectionable.
  - ✓ the user does not have the right to transmit.
  - ✓ infringes any patent, trademark, trade secret, copyright or other proprietary rights of any party
  - ✓ is unsolicited or unauthorised advertising, promotional materials, "junk mail," "spam," "chain letters," "pyramid schemes" etc.
  - ✓ contains software viruses or any other computer code, files or programs designed to damage computer software, hardware or telecommunications equipment.

- They also will not use the systems to:
  - ✓ impersonate any person or entity
  - ✓ interfere with or disrupt the service or servers or networks connected to the service, or disobey any requirements, procedures, policies or regulations of networks connected to the service.
  - ✓ collect or store personal information about others without direct reference to The Data Protection Act.
  - ✓ undertake any trading, gambling, other action for personal financial gain, or political purposes unless as part of an agreed curriculum project.
  - ✓ store or use any unauthorised software.

4. File storage

4.1 Files will be stored either on a school or BPET provided system with appropriate file-security, on a BPET approved network file store or, by prior agreement on a third-party system which meets the basic security requirements agreed by the Trust.

4.2 This includes the use of external USB storage of any kind which may not be used on any Trust IT system without previous written authorisation from the Director of Operations.

4.3 Files should never be stored on a public-access file store system not approved by BPET. Any sensitive information to be emailed or otherwise transmitted outside the school or BPET must be encrypted to a standard agreed in advance with IT support.

4.4 There are various cloud services in use by BPET. Staff are required to only use those services that are supported by the Trust, secured by their business login (either @bpet.co.uk or @academyname.co.uk or @rivermead.wokingham.sch.uk) and have a relevant Data Sharing Agreement in place.

4.5 Trust email accounts should not be used to sign up or login to services that are solely for personal use, such as personal shopping accounts or personal mailing lists.

4.6 It is not acceptable under any circumstances to use a personal cloud storage account (e.g. a personal Dropbox) to handle BPET data.

4.7 **Digital and video images:** Although it is recognised that there will be some variation in the approach taken by different schools to the taking and use of digital and video images of pupils, the majority of points noted below should feature in most school policies. Where the school chooses to vary from the guidelines, they should have clearly thought through the reasons for doing so, made this clear in their policy, ensured consistency with other policies such as Safeguarding, and informed all those concerned.

- Parental permission:
  - The school will ensure that appropriate written permissions are obtained for the taking and use of digital and video images of pupils. Such use could include the school website, learning platform or social media; display material in and around the school or off site; the school prospectus or other printed promotional material; local/national press.
  - If specific individual pupil photographs are to be used publicly, such as on the school website, in the prospectus or any other high profile publication, then a check should be made with individual parents for this additional use.

- Unless specific parental permission has been obtained, pupils will not be identified by name in any title or commentary accompanying digital or video images that is in the public domain. The school will also ensure that pupil names are not used in any file names used to save images; or in tags when publishing online.
- Where parental permission has not been obtained, or it is known that a pupil should not be photographed or filmed, every reasonable effort should be made to ensure that a pupil's image is not recorded.

- Storage and deletion:
  - All images of pupils will be securely stored in one central location.
  - Where memory cards, USB drives, CDs or cloud storage are used during the process of capture or transfer, this must only be for temporary storage until images can be uploaded to the secure central location. The images should then be deleted from the temporary storage location and care taken to ensure they are not still available, e.g. in a recycle bin.
  - Images of pupils should normally be deleted once a pupil has left the school unless being kept as part of archived records. Such retention, and the period involved, should be specified in the Data Protection or Data Retention policy.
- Recording of images:
  - All staff and pupils must sign the ICT Acceptable Use Agreement.
  - School digital devices should always be used to record images of pupils (subject to any variation the school agrees as noted below in 'Use of staff personal devices').
  - All pupils appearing in images should be appropriately dressed.
  - Pupils must not take, use, share, publish or distribute images of others without their permission.
  - Where images are taken using devices with a facility to store or transfer data to other locations (e.g. automatic copying to online 'cloud' storage) care must be taken that the location of images of pupils is clearly understood and in line with ICO (Information Commission's Office) guidance.
  - All digital devices capable of taking photographs and recording sound or video, whether belonging to the school or personal, may be subject to scrutiny if required.
  - Where volunteers are supporting school staff, they should abide by the same rules as school staff as far as is reasonable.
- Use of staff personal devices:

  It is recognised that the most straightforward approach is not to allow use of staff personally owned devices (e.g. staff smartphones, personally owned cameras) to record images. Where a school wishes to vary from this, e.g. for off-site activities, the following should apply:
  - It will be clearly understood under what circumstances it is permissible to use a personal device.
  - Images will be transferred to a secure location on the school's system as soon as possible and the originals/any copies deleted.
  - Such staff personal devices should be passcode protected.
- Parents taking photographs or video:

  Where the school chooses to allow the recording of images at 'public' events the following should apply:
  - Images may only be recorded for personal use and can only be shared with immediate family and friends. They must not be shared on social networking sites or other websites that are accessible by the general public.
- Events/Activities involving multiple schools:
  - When taking part in events organised by other schools or organisations, e.g. sports or music events, the schools involved will consider what image guidelines should apply.
  - For larger events it is reasonable to expect that specific image guidelines should be in place. Where relevant these should include reference to press images.
  - Consideration should be given as to how those attending the event will be informed of the image guidelines that apply, e.g. a letter before the event, announcement at the event, or information in any printed programme.

- Although the school will make reasonable efforts to safeguard the digital images of pupils, parents should be made aware that at some types of event it is not always realistic to strictly enforce image guidelines. The school cannot therefore be held accountable for the use of images taken by parents or members of the public at events.

4.8 Electronic devices - search and deletion:

- Schools can search pupils for items 'banned under the school rules' and has the power to 'delete data' stored on seized electronic devices. Clear guidelines relating to this should be communicated to staff and parents. Such guidelines will include:
  - Details of which items are banned under the school rules and may be searched for
  - A list of staff members/roles authorised to examine and/or erase data on electronic devices
  - Clear guidance as to what is, and is not, allowed when searching a pupil
  - When data will be deleted or kept as evidence
  - How incidents will be recorded

4.9 Backup and disaster recovery:

- The school will define and implement a backup regime which will enable recovery of key systems and data within a reasonable timeframe should a data loss occur. This regime should include:
  - The use of a remote location for backup of key school information, either by daily physical removal in an encrypted format, or via a secure encrypted online backup system.
  - No data should be stored on the C drive of any curriculum computer as it is liable to be overwritten without notice during the process of ghosting the computers.
  - Staff are responsible for backing up their own data on teacher laptops/devices and should utilise any system that may be enabled such as automated copying of files to the school server.
  - Backup methods should be regularly tested by renaming and then retrieving sample files from the backup.
  - The school should also define a whole school ICT disaster recovery plan which would take effect when severe disturbance to the schools ICT infrastructure takes place, to enable key school systems to be quickly reinstated and prioritised, including who would be involved in this process and how it would be accomplished.

5. Internet services

5.1 BPET expects users to act responsibly in accessing the internet and to report any offending material to the relevant authority.

5.2 As staff may access the internet through a number of public and private routes it is essential that staff use their professional judgment for their use of the internet.

5.3 Accessing inappropriate material over the internet, either using BPET equipment, or during working hours is a serious disciplinary matter.

5.4 All users should be aware that as well as monitoring internet traffic to block content, the school deems unacceptable; our systems also watch for keywords listed by the Home Office (as part of the PREVENT strategy) and the Internet Watch Foundation to raise an alert when a pattern of communication is one that may be a cause for concern.

5.5 Internet access of all staff members & pupil will be monitored.

5.6 The school maintains and supports the managed filtering service provided by RM, the Internet Service Provider (ISP), and the South East Grid for Learning (SEGfL).

5.7 Changes to network filtering should be approved by the ICT Subject Leader and the ICT Technician/Network Manager. Any filtering issues should be reported immediately to the ISP and/or SEGfL.

5.8 The school will take all reasonable precautions through various filter systems 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. The school cannot accept liability for the material accessed, or any consequences of internet access.

5.9 Users must not create, download, upload, display or access knowingly, sites that contain pornography or other unsuitable material that might be deemed illegal, obscene or offensive.

5.10 Unauthorised users must not attempt to disable or reconfigure any filtering, virus protection or similar.

5.11 All pupils using the internet, and associated communication technologies, will be made aware of the school's e-Safety Guidelines. Pupils will receive guidance in responsible and safe use on a regular basis.

5.12 **Learning platform and/or website:**

- The school learning platform and/or website should include the school address, school e-mail, telephone and fax number including any emergency contact details.
- The school learning platform and/or website should be used to provide information and guidance to parents concerning e-safety policies and practice.
- Staff or pupils' home information should not be published.
- The copyright of all material posted must be held by the school or be clearly attributed to the owner where permission to reproduce has been obtained or given.

5.13 Mail services

- Information held in a BPET administered email system is the property of the BPET.
- All BPET staff that require email access as part of their duties will be provided with a business email address using the BPET approved service. The email address will either be @bpet.co.uk or the recognized email domain of their academy (eg @rivermead.wokingham.sch.uk).
- Personal email addresses must not be used to transact BPET business except in an emergency situation where a rapid response is required and the proper service is unavailable. When a personal address is used, a copy of the message must be sent to the relevant business address so that an audit trail is maintained.
- Emails of a confidential or sensitive nature must be clearly marked in the subject line so that the recipient is made aware. Sensitive information should be sent as an attachment rather than in the body of an email and the content of that email should be password protected.

5.14 Pupils and staff will be informed that the use of school e-mail or messaging accounts will be monitored.

5.15 Under no circumstances should users use e-mail to communicate material (either internally or externally), which is defamatory or obscene.

5.16 Pupils may only use approved e-mail or message accounts on the school system.

5.17 Pupils should immediately tell a staff member if they receive an offensive e-mail or message.

5.18 Pupils should not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone via an e-mail or message.

5.19 Pupils wishing to send e-mails to an external person or organisation must be authorised by a member of staff before sending.

5.20 Information of a sensitive nature should not be sent by unencrypted e-mail.

5.21 Media rights

- Many files that can be purchased or rented privately (music, films etc) have licenses that forbid their storage or transmission on a business network.
- Users will never use media they have purchased on our systems without being absolutely certain they are not violating the license agreement they made with the owner.

5.22 Security

- Each user will be given a unique ID and password that will allow them to access their account. The ID and password are solely the responsibility of the user and not to be shared with other users or third parties for any reason.
- Pupils may have a group password or individual passwords for accessing the network. All users will have an individual log on to the learning platform and/or secure areas of the website.
- Clear guidelines will be provided for all users which explain how effective passwords should be chosen. Further expectations of users are detailed below:

- ✓ No individual should tell another individual their password.
- ✓ No individual should log on using another individual's password, unless they are a member of staff logging on as a pupil.
- ✓ Once a computer has been used, users must remember to log off so that others cannot access their information.
- ✓ Users leaving a computer temporarily should lock the screen (Windows key + L).
- ✓ Passwords should be changed at regular intervals. The school may choose to enforce this requirement.
- ✓ In the event that a password becomes insecure then it should be changed immediately.

- All information about staff and students will be dealt with in compliance with the Data Protection Act and only given to authorised agencies.
- BPET reserves the right to monitor all traffic (email and files) on the network, either manually or through automated software, to ensure statement compliance and to aid in resolving any issues.
- Children should always be supervised by a member of staff when they are using laptops/IT devices in school at all times.
- The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that procedures outlined within this policy are implemented by those responsible.
- School ICT technical staff may monitor and record the activity of users on the school ICT systems and users will be made aware of this.
- Servers, and communications cabinets should be securely located and physical access restricted.
- Wireless systems should be secured to at least WPA level (Wi-fi protected access).
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Technician/Network Manager.
- Access to the school ICT systems will cease when a pupil leaves or, in the case of a member of staff, ceases to be employed by the school.
- Staff laptops/devices and flash drives are likely to be taken out of school and may well contain sensitive data. Schools should encrypt staff laptops and staff should only use school provided encrypted flash drives.
- The following security measures should also be taken with staff laptop/devices:
  - ✓ Laptops/devices must be out of view and preferably locked away overnight whether at school or home.
  - ✓ Laptops/devices should never be left in a parked car, even in the boot.
  - ✓ Laptops/devices should not be used for purposes beyond that associated with the work of the school, e.g. by the family of a member of staff.
  - ✓ Where others are to use the laptop, they should log on as a separate user without administrator privileges.
- Loading/installing software
  - ✓ For the purpose of this policy, software relates to all programs, images or screensavers, which can be downloaded or installed from other media.
  - ✓ Any software loaded onto the school system or individual computers and laptops/devices must be properly licensed and free from viruses.
  - ✓ Only authorised persons, such as the ICT Technician/Network Manager or ICT Subject Leader, may load software onto the school system or individual computers.
  - ✓ Where staff are authorised to download software to their own laptops/devices they must ensure that this is consistent with their professional role and that they are satisfied that any downloaded images and video clips do not breach copyright.

6. E-Security

- The head teacher is the Senior Information Risk Officer (SIRO), and is responsible for: Implementing effective strategies for the management of risks imposed by internet use, and to keep its network services, data and users secure; Establishing a procedure for managing and logging incidents; Making any necessary changes to this policy and communicating these to all members of staff.
- The IT technician is responsible for the overall monitoring and management of e-security. All members of staff and pupils are responsible for adhering to the processes outlined in this policy, alongside their school's E-safety Policy and IT Code of Conduct/Acceptable Use Policy.
- The School ensures staff know to immediately report, and who to report to, any incidents where data protection may have been compromised, such as when passwords for sensitive systems or devices are lost or stolen, so that relevant action(s) can be taken.
- All staff are DBS checked and records are held on the school's central record register. We ensure members such as staff and volunteers sign an IT Code of Conduct - Acceptable Use Agreement Form.
- Governing Body will: Hold regular meetings with the head teacher and IT Technician to discuss the effectiveness of e-security; Review and evaluate policies related to E-security on a termly basis in accordance with the head teacher and IT technician, taking into account any incidents and recent technological developments.
- The school uses the DfE S2S site to securely transfer CTF pupil data files to DfE / other schools.
- Uses the Wokingham Borough Council Admissions system to transfer admissions data.
- Stores any Protect and Restricted written material in appropriate storage.
- Ensures all servers are in lockable locations and managed by DBS-checked staff.
- Uses remote secure back-up for disaster recovery on our network, curriculum and admin server(s).
- Complies with the WEEE directive on equipment disposal, by using an approved disposal company for disposal of IT equipment. For systems, where any protected or restricted data has been held, (such as servers, photocopiers), we get a certificate of secure deletion.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using a shredder, or placed into confidentiality bags which are collected by Select Services.
- The School has an approved educational web filtering across our wired and wireless networks. It also has an additional layer of monitoring software across our network system. It has monitoring of school e-mails / blogs / learning platforms, etc.
- Makes clear all responsibilities and expectations with regard to data security.
- Ensures all staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private.
- Expects staff to undertake house-keeping checks termly to review, remove and delete/destroy any digital materials and documents which need no longer be stored.
- Require staff to log-out of systems when leaving their computer.
- Managing User Privileges: The school understands that controlling what users have access to is important for promoting network security. User privileges will be differentiated, i.e. pupils will have different access to data and the network from members of staff. The head teacher will clearly define what users have access to and will communicate this to the IT technician, ensuring that a written record is kept. The IT technician will ensure that user accounts are set up appropriately such that users can access the facilities required, in line with the head teacher's instructions, whilst minimising the potential for deliberate or accidental attacks on the network. The IT technician will ensure that websites are filtered on a weekly basis for inappropriate and malicious content. Any member of staff or pupil that has accessed inappropriate or malicious content will be recorded. All users will be required to change their passwords on a regular basis and must use upper and lowercase letters, as well as numbers, to ensure that passwords are strong. Users will also be required to change their password if this becomes known to other individuals. Pupils are responsible for remembering their passwords. However, the IT technician will have an up-to-date record of all usernames and passwords and will be able to reset them if necessary. Pupils in key stage 1 will not have

individual logins and class logins will be used instead. If it is appropriate for a pupil to have their individual login, the IT technician will set up their individual user account, ensuring appropriate access and that their username and password is recorded.

- Secure Configuration: An inventory will be kept of all IT hardware and software currently in use at the schools, including mobile phones and other personal devices provided by the school. This will be audited on a regular basis to ensure it is up-to-date. Any changes to the IT hardware or software will be documented using the inventory, and will be authorised by the IT technician before use. All systems will be audited on a regular basis to ensure the software is up-to-date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security, and will be recorded on the inventory. Any software that is out-of-date or reaches 'end of life' will be removed from systems, i.e. when suppliers end their support for outdated products, such that any security issues will not be rectified by suppliers.
- All hardware, software and operating systems will require passwords for individual users before use. Passwords will be changed on a termly basis to prevent access to facilities which could compromise network security. The school believes that locking down hardware, such as through strong passwords, is an effective way to prevent access to facilities by unauthorised users.
- Network Security School : Rivermead employ firewalls in order to prevent unauthorized access to the systems. These will be deployed as a "localized deployment" whereby the broadband service connects to a firewall that is located on an appliance or system on the school premises, as either discrete technology or a component of another system. As the school's firewalls are managed on the premises, it is the responsibility of the IT technicians to effectively manage the firewall.
- The IT technician will ensure that: The firewall is checked regularly for any changes and/or updates, and that these are recorded using the inventory; Any changes and/or updates that are added to servers, including access to new services and applications, do not compromise the overall network security; The firewall is checked regularly to ensure that a high level of security is maintained and there is effective protection from external threats; Any compromise of security through the firewall is recorded using an incident log and is reported to the head teacher.
- The IT technician will react to security threats to find new ways of managing the firewall. Staff have secure area(s) on the network to store sensitive documents or photographs. The staff are required to log-out of systems when leaving their computer, but also enforce lock-out after 30 mins when computers have been inactive.
- The school uses encrypted flash drives if any member of staff has to take any sensitive information off site.
- The school uses Microsoft 365 based services for online (non-sensitive) document storage, and use an appropriate solution with authentication for remote access into our systems.
- The School requires that any Protect and Restricted material must be encrypted if the material is to be removed from the school, and limit such data removal.
- There is an approved remote access solution so staff can access sensitive and other data from home through school provided IT equipment.
- School staff are set up with usernames and passwords for e-mail, network access, and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- Types of Attack
    - Malicious Technical Attacks: Intentional attacks which seek to gain access to a school's system and data. Often, these attacks also attempt to use the school's system to mount further attacks on other systems, or use the system for unauthorised purposes, and can lead to reputational damage.
    - Accidental Attacks: These attacks are often as a result of programme errors or viruses in the school system. Whilst these are not deliberate, they can cause a variety of problems for schools.
    - Internal Attacks: These attacks involve both deliberate and accidental actions by users and the introduction of infected devices or storage into the school's system,

e.g. USB flash drives.
    - Social Engineering: Attacks resulting from internal weaknesses which expose the school's system, e.g. poor password use.
- Incidents: In the event of an internal attack or any incident which has been reported to the IT technician, this will be recorded using an incident log and by identifying the user and the website or service they were trying to access. All incidents will be reported to the head teacher, who will issue disciplinary sanctions to the pupil or member of staff, in accordance with the processes outlined. If necessary, the management of e-security will be reviewed to ensure effectiveness and minimise any further incidents.
- In the event of any external or internal attack, the IT technician will record this using an incident log and respond appropriately, e.g. by updating the firewall, changing usernames and passwords, updating filtered websites, centralised deployments (Trust) etc.
- In the event of any external or internal attack, the IT technician will record this using an incident log and will contact the third party provider to ensure the attack does not compromise any other schools' network security. The IT technician will work with the third party provider to provide an appropriate response to the attack, including any in-house changes.
- Removable Media Controls and Home Working : The schools understand that pupils and staff may need to access their school network from areas other than on the premises. Effective security management will be established to prevent access to, or leakage of, data, as well as any possible risk of malware.
- The IT technician will encrypt all school-owned devices for personal use, such as laptops, USB sticks, mobile phones and tablets, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.
- Pupils and staff are not permitted to use their personal devices where the schools shall provide alternatives, such as work laptops, tablets and USB sticks, unless instructed otherwise by the head teacher. If staff are instructed that they are able to use their personal devices, they will ensure that they have an appropriate level of security and firewall to prevent any compromise of the school's network security. This will be checked by the IT technician. When using laptops, tablets and other portable devices, the head teacher will determine the limitations for access to the network, as described in the section of this policy relating to user privileges. Staff who use school-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off of the school premises.
- The IT technician will apply filtering regarding the use of websites on these devices, in order to prevent inappropriate use and external threats which may compromise the network security when bringing the device back onto the premises.
- All data will be held on systems centrally in order to reduce the need for the creation of multiple copies, and/or the need to transfer data using removable media controls.
- The Wi-Fi network at the schools will be password protected. Staff and pupils are not permitted to use the Wi-Fi for their personal devices, such as mobile phones or tablets, unless instructed otherwise. A separate Wi-Fi network will be established for visitors at the schools to limit their access from printers, shared storage areas and any other applications which are not necessary.
- Malware Prevention : The schools understand that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media controls. The ICT technician will ensure that all school devices have secure malware protection, including regular malware scans, and will update malware protection on a termly basis to ensure they are up-to-date and can react to changing threats. Malware protection will also be updated in the event of any attacks to the school's hardware and software. Filtering of websites, as detailed elsewhere in this policy, will ensure that access to websites with known malware is blocked immediately and reported to the IT technician. The schools will use mail security technology, which will detect and block any malware that is transmitted by email. This will also detect any spam or other messages which are designed to exploit users. The IT technician will review the mail security technology on a termly basis to ensure it is kept up-to-date and is effective.
- User Training and Awareness : The IT technician and head teacher will arrange training for

pupils and staff on a regular basis to ensure they are aware of how to use the network appropriately in accordance with the IT Code of Conduct/Acceptable Use Policy. Training will also be conducted around any attacks that occur and any recent updates in technology or the network. All staff will receive training as part of their induction programme, and any new pupils joining the schools will also receive appropriate instruction.

7. Using social media

- When using social media, professionally or privately, staff should ensure that content associated with them is consistent with your work at BPET - use professional discretion in all personal communications in social media, use a disclaimer if using social media for personal purposes, and do not use BPET e- mail address, logos or other identification, making it clear that what you say is representative of personal views only.
  - ✓ Staff have a perfect right to use social networking sites in their private life. In doing so they should ensure that public comments made on social networking sites are compatible with their role as a member of staff and that they show the highest standards of professional integrity.
- Connection with students through social media should only take place with a clear purpose agreed in advance with the Headteacher.
- Pupil use of social networking should conform to age restrictions and will not be allowed in school unless this is part of an educational activity and has been authorised by an appropriate member of staff.

8. Accessing school or BPET data off premises

i. When BPET make access to systems available offsite, the member of staff accepts responsibility to ensure that nobody other than the authorised person gains access to the system (not leaving a PC logged in and unattended at home for example).
ii. All school-related cloud based services (such as Arbor, PurpleMash, Mathletics, Century, Edukey and any other current & future cloud based services) should only be accessed by school provided IT devices.

9. Care of equipment

i. Equipment is provided for the purpose of carrying out your duties and must always be looked after with care.
ii. Either at the end of the period of employment with BPET, for servicing or for replacement, staff will be asked to return equipment.
iii. BPET reserves the right to charge the replacement cost of any lost items such as power supplies or cables that are required to reallocate the equipment to another user.

10. Data Protection

i. All staff are responsible for ensuring that at all times they handle data with proper care and respect for the rights of our colleagues and the people we work with in accordance with the BPET Data Protection Policy.
ii. All users are responsible for only accessing, altering and deleting their own personal files. They must not access, alter or delete files of another user without permission.
iii. Sensitive data is any data which links a pupil's name to a particular item of information and/or the loss of which is liable to cause individuals damage and distress. Therefore, such

data:

1. must be encrypted on laptops/devices and any other removable media;
2. should not be e-mailed between staff;
3. should be deleted from laptops/devices at the end of an academic year or earlier if no longer required.

iv. Staff should take care not to leave printed documents with sensitive information open to view, e.g. by not collecting them promptly from printers, or leaving such documents on open desks. Sensitive information should be held in lockable storage when office staff are not present.

v. There must be clear procedures for the safe and secure disposal of any device that records data or images, e.g. computers, laptops, memory sticks, cameras, photocopiers, etc.

11. Computer security

i. IT Support must ensure that all systems made available to staff use networks with appropriate firewall protection, virus checking must be installed on all computers and operating systems must be kept updated with security patches. All computer systems, including staff laptops/devices, should be protected by an antivirus product which is preferably administered centrally and automatically updated. The antivirus product should allow for on-access scanning of files which may be being transferred between computers or downloaded from the internet. In the latter case only, dependable sources should be used.

ii. Staff have the responsibility not to tamper with or circumvent those systems and inform IT support if they believe their system is at risk.

iii. Systems must be set up to allow staff access only to the information they need to do their job.

iv. Staff should never share access to accounts and never share passwords. Where several people need to access a common account (eg an enquiries email address) it must be set up so that either one person monitors the account and informs colleagues, or as an alias where multiple members of staff receive communication from the shared address. It is the responsibility of the technical support and management staff in each academy to be aware of the potential for any kind of informal arrangement where passwords are shared and stop them.

v. Staff user accounts maybe be setup or transferred to Multi Factor Authentication (MFA) at any point as directed by the BPET Operations Team. This is an added layer of security to BPET accounts. It is the priority for all staff accounts to be setup with MFA, where possible, for any access to BPET based systems.

vi. In cases where an account falls dormant, either because someone has left employment with the BPET or is absent long-term, arrangements put in place must not compromise data security.

vii. Any personal information held electronically that would cause damage or distress if it were lost or stolen must be encrypted (eg within a secure management information system or password protected file)

viii. Local storage of computer systems used to retain any business data (eg computer hard disc) must be encrypted. Where an operating system is being used that does not support this as standard, a strong encryption alternative must be installed.

ix. Regular back-ups of the information on computer systems must be taken and copies kept in a separate place. Under normal circumstances this is arranged by IT Support, however staff should ensure they are confident that important files are being backed up correctly. All information must be securely erased before disposing of old computers (through the use of secure erasure software or physical destruction of the hard disk).

x. Only authorised persons, such as the IT Technician or IT Service provider may load authorized software onto the school system or individual computers.

12. Transferring data away from computer systems

i. Moving data between systems is one of the highest risk activities in terms of data protection and special care should always be exercised.
ii. The preferred method for moving data is either through the use of the BPET email system, or the approved cloud storage systems within BPET.
iii. External drives (such as USB pen drives) are not to be used and can only ever be used under the direct supervision of the IT Support team, who will ensure encryption is enabled, or with written permission from the Data Protection Officer, setting out the scope and limitations on use.

13. Mobile devices

i. Mobile devices also pose a security risk, in particular of "passive loss" of data where a colleague has a smart phone or tablet set up to receive business email or store files in some way.
ii. To minimise risk, any mobile device to be configured with a business email address must have a PIN lock enabled, if that is not possible then a business email address should not be used with that device. Staff must be aware that deliberately setting up access to their business email on an insecure device without taking steps to protect it is in breach of Trust Acceptable Use Policy.
iii. If a device holding BPET data (including email) is lost, BPET IT Support provider must be informed immediately to allow us to remotely wipe any sensitive data from the device.
iv. Technical support staff in each school will seek to authorise mobile devices on the BPET servers, so that if a device is lost or stolen it can be remotely wiped.
v. Pupils will not be allowed to bring mobile phones to school unless prior arrangements are made with the school.
vi. Where mobile phones are allowed in school they may not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or images is forbidden.
vii. Pupils will not be allowed to bring in games devices, particularly those which allow ad hoc networks to be established.
viii. Teacher/parent contact should normally be by the main school telephone and not via a mobile device except where off-site activities dictate the use of a mobile phone.
ix. Parent helpers in school and staff must ensure that they do not send personal messages, either audio or text, during contact time with pupils. If an exceptional emergency arises they should arrange temporary cover whilst they make a call.
x. Staff and pupils may send educational messages during lesson times if these are part of the curriculum.
xi. Schools should be vigilant where mobile phones are used with children in the Foundation Stage. Staff, helper and visitor mobile devices may normally be switched off or on silent during the times that children are present.
xii. No device in any of the school buildings should contain any content that is inappropriate or illegal.
xiii. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
xiv. E-Safety Education
    - Learning and teaching for pupils
        - ✓ Pupils should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
        - ✓ Pupils should be helped to understand the need for an Acceptable Use Policy and, depending on age, asked to sign to indicate agreement.
        - ✓ Pupils should be taught to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
        - ✓ Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

- ✓ Key e-safety messages will be included within the curriculum and reinforced as part of a planned programme of assemblies and other appropriate opportunities.
- Staff training
  - ✓ Staff will be kept up to date through regular e-safety training.
  - ✓ Staff should always act as good role models in their use of ICT, the internet and mobile devices.
- Parental support - The support of, and partnership with, parents should be encouraged. This is likely to include the following:
  - ✓ Awareness of the school's policies regarding e-safety and internet use; and where appropriate being asked to sign to indicate agreement.
  - ✓ Practical demonstrations and training
  - ✓ Advice and guidance on areas such as filtering systems , educational and leisure activities , suggestions for safe internet use at home

14. Reporting and Consequences of Non-Compliance

i. Non-compliance with this policy may lead to disciplinary action being taken.

15. Policy Status

i. This policy does not form part of any employee's contract of employment.

16. Related Policies

i. This policy is related to the following other BPET policies:
   1. Data Protection Policy

17. Monitoring and review

i. This policy is reviewed every two years by the BPET Board. Any changes to this policy will be communicated to all relevant stakeholders.

Rivermead Primary School

Staff Code of Conduct for ICT

To ensure that staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications, including email, IM and social networking are compatible with my professional role and messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Rivermead Primary School Staff Code of Conduct for ICT.

Signed: …… Name: …… Date: ……

Accepted for school: …….. Name: ……..