Riverside Primary School

Computer Security Policy

September 2022

Reviewed

Review and Monitoring
Our policy has been carefully reviewed.

Riverside Primary School
Computer Security Policy

Virus
Anti-virus – All PCs and laptops must be protected with anti-virus software, which will need to be updated regularly.

All users of information technology equipment should be aware of the virus threat.

Virus Outbreaks – can occur through opening emails, computer downloads, removable data storage transferred between machines etc.

Software supplies must be obtained from reputable suppliers.

All detected viruses must be reported to the ICT co-ordinator at an appropriate time.

The following measures must be taken if there is a suspected virus outbreak:

- Switch off the PC
- Contact the ICT co-ordinator
- Contact IT Solutions (Paul Greatbatch)

No computer equipment or media may be taken out of the area where the outbreak occurs, until the virus is removed.

Content Filtering
All networked PCs, laptops and iPads are protected by Councils content filtering.
iPad filtering:
Settings, wifi, HTTP proxy, manual. Server: 10.100.12.140, Port: 8080.

Microsoft Updates
All PCs and laptops should have regular Microsoft security updates carried out. iPads will regularly be updated by It Solutions using Mac Book Air.

Passwords
All staff will be allocated passwords, which should be kept confidential. All laptops are configured with strong password controls to protect against unauthorised access, with use limited to teaching staff only. The ICT co-ordinator will set passwords which should be changed by member of staff as appropriate.
Staff laptops have two separate passwords with two separate accounts. One account will be for school use and the other for home use. All USB drives should be password protected. Any confidential data should be saved onto a password secure USB memory drive. The ICT Co-ordinator will issue all staff

with a USB memory drive. Any problems or difficulties should be reported to the ICT Co-ordinator.

Passwords should:

- Be no less than 8 characters in length.
- Avoid obvious personal references.
- Use mixed numeric and alphabetic characters where possible.
- Not be the same as or similar to the username or previous password.

All documentation containing passwords should be securely filed.

There are no circumstances under which a personal password should be revealed to any other person. Anyone who is entitled to use a system has their own login and password and they do not need access to anyone else's. Visitors and Students have their own logins and passwords and therefore do not need to use a member of staffs. Please see the ICT co-ordinator for visitor and student logins and passwords. No child should be given access to any locked areas or given codes, passwords or keys.

All PC's, laptops and ipads must be locked using ctrl, alt, delete when not in use or when the user leaves the room.

School's Social Media

Riverside Primary School has a School Twitter account and Facebook page (Riverside Primary@ Mintonlane) for sharing information (@RiversideNS1). Individual classes also have a Twitter account for sharing information, news and photographs. Parents must be accepted by users to access information.

Access

All class teachers have access to individual class pages. Mrs Angela Yilmaz (Head Teacher) and Miss Charlotte Embleton (co-ordinator) have access to whole school account.

Content of Accounts

Weekly learning activities, songs, rhymes and children's work will be shared with parents and carers via the Twitter page. Photographs of children will only be used with prior permission from parents and carers.

Prohibited content: Children who have not received permission for photographic use on school's social media site will not have any images posted on Twitter or Facebook – seek information from school office.

Communication and Contact

No parents or pupils will be able to post, upload or tweet directly onto the school's Twitter account. All posts will be made by named staff. Twitter account will be set for 'viewing use only'.
Facebook account will include ability to post, like and comment. All posts made will be regularly monitored and swift action will be taken in the case of any inappropriate content. Advice sought by Neil Brown.

Staff Protocol
All staff at all times must act in the best interests of the children when using social media.
Staff must not post any content that may cause the school unwelcome publicity or bring the school or its employees into disrepute.

All IPADS and laptops including the hall laptop must be replaced correctly into the storage trolleys and charging leads plugged in. All trolleys must be returned to the ICT suite and plugged into the mains socket for charge at the end of the school day. Nigel Bexon (Caretaker) will take responsibility for ensuring ICT equipment is locked away securely at the end of the school day.

The ICT cupboard must be locked at all times. No child should be given a key to any locked areas at any time.

No information/files/data (where a child's identity could be accessed) should be saved onto the desktop or drive of any of the laptops. The 'shared drive' is the only place where such data is stored.

User base
The school user base will be reviewed regularly to ensure only existing employees have access to the network. Leaver accounts should be deleted in a timely manner. All staff will be given their own login and password for using the computers.

Monitoring Web Logs
Ranger web logs will be examined weekly by the ICT Technician.

Data Back Up
Network back ups are carried out at the end of the school day. A physical check should be carried out daily, to ensure the back up has completed successfully.
Please note: All computers automatically turn off at 6:00pm for the evening. Please ensure that any documents which you are working on at this time are saved before the system shuts down.

Staff using laptops should ensure that any data is backed up to a removable device (USB password protected memory stick), rather than saved on the hard drive. Any critical data should then be saved to the server.

Disposal of ICT Assets
When the school curriculum ICT assets are earmarked for disposal, the corporate ICT service should be contacted to seek guidance and to determine the course of action.
When hardware is safely disposed of a certificate of proof should be issued by the company. A copy of this certificate will be kept by the ICT co-ordinator and

by Katy Taylor (Administrative Manager). Company used to safely dispose equipment: recycle@rrit.co.uk

Updates

It is the responsibility of the class teacher to ensure that any stand-alone computers or other ICT hardware in their room is updated regularly. Anti-virus software and Windows updates can be carried out quickly and easily if updated frequently. Laptops will be collected in each term and updated by the ICT Technician.

Review Date: September 2024