Redhill Primary Academy

Data Security Policy

Signed

Ms Fiona Seddon

Chair of Governors

Spring 2023

Redhill's Data Security Policy

Acceptable Use Agreement: Staff

Staff must sign this agreement digitally when they log on for the first time, then periodically afterwards. Failure to sign forces the computer to log the user off. Staff are aware of the schools AUP policy, as Senso prompts them to sign the above on logon.

Computer Viruses

- All files downloaded from the Internet, received via email or on removable media (e.g. CD, USB sticks) must be checked for any viruses using school provided anti-virus software (Sophos) before using them. Never interfere with any anti-virus software installed on school IT equipment that you use.
- Never remove school installed anti-virus from your computer – even to replace with your owned preferred software. Sophos actively quarantines downloads by sending them to a sandbox environment. There, it carries our rigorous testing before either denying or allowing the download.
- If you suspect there may be a virus on any school IT equipment, stop using the equipment and contact your IT technician immediately. They will advise you what actions to take and be responsible for advising others that need to know.

GDPR – Clear desk guidance

Staff must ensure they maintain a clear desk as this supports security, cleanliness and allows others to adopt any available space. By adopting this strategy, it will help reduce the risk of unauthorised access to sensitive and confidential data.

- Staff must always ensure their computer is always locked when it is unattended.
- This can be done through pressing the Windows + L key on the keyboard
- BitLocker: Each device has their own BitLocker password to access their device. If for whatever reason a member of staff forgets or loses their code; they will need to inform IT, who can then use a recovery key to allow access to the device.
- Staff should be mindful of the data they are accessing via cloud services such as OneDrive when not on a device with BitLocker or configured by the school.

Data & Device Security

The accessing and appropriate use of staff and child data is something that the school takes very seriously.

Security

- The school gives relevant staff access to its MIS system - Arbor
- It is the responsibility of everyone to keep passwords secure.
- Passwords are not to be written down under any circumstances .
- Staff are aware of their responsibility when accessing school data.
- To minimise the possibility of a data being lost or stolen, staff should refrain from the use of USB sticks and instead look to utilise OneDrive & Office 365 for data mobility.

By exception only, a USB stick maybe used provided it has been encrypted. In these cases the data placed on this device should not be sensitive.

- None encrypted USB sticks are strictly prohibited.
- Where necessary the IT technician will Bitlocker the USB stick. Staff do not have to buy pre-encrypted ones.
- Staff are required to avoid leaving any portable IT equipment unattended. This includes, but is not limited to, Laptops, Phones, USB Sticks. Where this is not possible, equipment should be secured and out of sight.
- Staff should always carry portable IT equipment as hand luggage and keep it under their control.
- It is the individuals responsibility to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed.

Protective Marking

Appropriate labelling of devices should help the school's secure data and so reduce the risk of security incidents. Your IT technician will ensure all devices are securely marked to identify the school as the owner of all digital devices. They will also be labelled with the appropriate PC ID number that will also be reflected on the school's IT Audit.

On secure digital devices, ensure the owner information is filled in to include the staff members' last name, the school name and main phone number. This does not put the device at risk but increases the chances of it being returned to the school if misplaced or stolen. If an attempt is made to access the devices illegally, they will erase themselves.

Disposal of Redundant ICT Equipment Policy

- All redundant IT equipment is disposed of through PRM. This includes a written receipt for the item including all asset model and serial details. All receipts are kept digitally for reference.
- Any redundant IT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate – Equipment in IT office.
- Disposal of any ICT equipment will conform to:
    - The Waste Electrical and Electronic Equipment Regulations 2006
    - The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
    - Data Protection Act 1998
    - Electricity at Work Regulations 1989
- The school will maintain a comprehensive inventory of all its IT equipment (yearly audit) including a record of disposal
- The school's disposal record will include:
    - Date item disposed of
    - Authorisation for disposal, including:
    - Verification of software licensing
    - Personal data likely to be held on the storage media *
    - How it was disposed of e.g. waste, gift, sale
    - Name of person & or organisation who received the disposed item

* *If personal data is likely to be held, the storage media will be over written multiple times to ensure the data is irretrievably destroyed.*

Email

The use of email within the school is an essential means of communication for staff. In the context of school, email should not be considered private.

Managing email

- The school gives all staff their own email account to use for all school business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed
- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. School systems monitor all email content using Becta advised procedures. The school email account should be the account that is used for all school business.
- Under no circumstances should staff contact students, parents or conduct any school business using personal email addresses
- Under no circumstances should a member of staff, whose personal device is set to receive emails, allow that device to be used by any other user member of staff
- The school requires a standard disclaimer to be attached to all email correspondence, stating that:

  > *This email and its attachments may be confidential and are intended only for the authorised recipients of the sender. The information contained in the email and any attachments must not be published and copied and disclosed or transmitted in any form to any person or entity unless expressively authorised by the sender. If you have received this email in error you are requested to delete it immediately from your inbox and deleted items and advise the sender by return e-mail.*

- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Children may only use school approved generic accounts on the school system and only under direct teacher supervision for educational purposes
- Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your email account as follows:
  - Delete all emails of short-term value
  - Organise email into folders and carry out frequent house-keeping on all folders and archives
  - The forwarding of chain letters is not permitted in school irrespective of content
  - Staff must inform the Head teacher if they receive an offensive email
  - However you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply
  - The use of Hotmail, Yahoo, BTInternet, AOL or any other Internet based webmail service for sending, reading or receiving business related email is not permitted for students. For staff external email use, see **Personal, Sensitive, Confidential or Classified Information**.

Sending emails

- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section emailing **Personal, Sensitive, Confidential or Classified Information**
- Use your own school email account so that you are clearly identified as the originator of a message
- To encrypt an email, type the word encrypt with an opening/closing bracket at the start of the subject line.
- OneDrive should be used to share sensitive data as opposed to sending attachments. This prevents multiple copies of the same document being produced.
- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate
- Only send email to an entire group if the content of the communication is generally for the information of the group. To send to specific groups, use the 'mailto' section in Outlook to select from various distribution groups
- Do not send or forward confidential information to a school governor should their email address not be a school address.
- An outgoing email greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming email
- School email is not to be used for personal advertising

Sending Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using email - emailing confidential data is not recommended and should be avoided where possible
- Where your conclusion is that email must be used to transmit such data: obtain express consent from the IT technician to provide the information by email
- Exercise caution when sending the email and always follow these checks before releasing the email:
- Verify the details, including accurate email address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to email requests for information
- Do not send the information to anybody/person whose details you have been unable to separately verify (usually by phone)
- Send the information as an encrypted document attached to an email
- Provide the encryption key or password by a separate contact with the recipient(s) once you've received a conformation receipt/response.
- Do not identify such information in the subject line of any email
- Request confirmation of safe receipt

Receiving emails

- Check your email regularly
- Activate your 'out-of-office' notification when away for extended periods of time
- Never open attachments from an un-trusted source; Consult your IT technician first.
- Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

For added security when receiving emails the school has the following systems:

- Geo Blocking - Access to services outside of the UK is now prohibited without the use of a school laptop. This means phones tablets and laptops not provided by school are prohibited from connecting unless in the UK. The main reason for this particular measure is most compromises occur outside of the UK on non-school devices. This will stop third party access from abroad, should details be compromised.
- Auto forward block - Automatic rules to forward emails coming in to a school email box out of the organisation are now blocked. This stops third parties gaining mailbox access and forwarding mail to a third party email address automatically. You can still forward manually. But automation with a rule is prohibited

Passwords & Account\Password Security

Passwords

- Always use your own personal passwords to access computer based services
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff must change temporary passwords at first logon (no-one should be using the default Arbor password for example)
- Passwords need to be **Alpha-numeric –** They require 3 of the following - 1 uppercase, 1 lowercase, 1 number and/or 1 special character
- School issue iPads are to be given a 6 digit pin if they contain PII (Personal Identifiable Information) – An example would be if a school device were to contain a school email account, or a twitter account for example.
- Redhill's network will not allow the same password to be used again for another 3 cycles – It will remember the last 3 passwords used.
- Change passwords whenever there is any indication of possible system or password compromise
- Do not ever record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to the IT technician when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- User ID and passwords for staff and students who have left the school are removed from the system with immediate effect (for staff).
- If you think your password may have been compromised or someone else has become aware of your password report this to your IT technician immediately.

Password Security

- Password security is essential for staff, particularly as they are able to access and use children's data. Members of staff are expected to have alpha numeric passwords which are not to be shared with anyone, including other members of staff.
- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security. This is done through Senso.
- Members of staff are aware of their individual responsibilities to protect the security and confidentiality of Redhill's network.
- Due consideration should be given when logging into School pod to the browser/cache options (shared or private computer)
- In our school, all IT password policies are the responsibility of the Head teacher and all staff and children are expected to comply with the policies at all times

Zombie Accounts

Zombie accounts refer to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all staff user accounts are disabled at the end of their last day if employment has ceased.
- Prompt action on disabling accounts will prevent unauthorized access
- Regularly change generic passwords to avoid unauthorized access (Microsoft© advise every 42 days)

Personal Information Promise

The Information Commissioner's Office launched a Personal Information Promise in January 2009.

The Head teacher, on behalf of Redhill Primary School, promises that we will:

- value the personal information entrusted to us and make sure we respect that trust;
- go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;
- consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;
- be open with individuals about how we use their information and who we give it to;
- make it easy for individuals to access and correct their personal information;
- keep personal information to the minimum necessary and delete it when we no longer need it;
- have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;
- provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or don't look after personal information properly;
- put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises; and
- regularly check that we are living up to our promises and report on how we are doing

Personal or Sensitive Information
Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared photocopiers are used within the school – sensitive and confidential information being duplicated must be seen only by the intended recipients.
- Only download personal data from systems if expressly authorised to do so by your manager

- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
- Where your computer is connected to a data projector or touch panel, you must 'freeze' or turn of the display if it risks compromising any security or data protection legislation.
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling
- Ensure removable media is purchased with encryption:
- Secured removable media is available from the school IT technician.
- The media (USB Flash Drives) requires a dual-case, alphanumeric password such as 'H@ppy321'
- Lost or stolen drives must be reported to your IT department immediately
- Data stored on the drives must be regularly backed up in a secure location (IE network shared drive) this is because;
- Should a school encrypted device be accessed illegally (via means other than password entry) the device will secure erase itself to protect the data.
- If lost the data is not recoverable
- Store all removable media securely
- Encrypt all files containing personal, sensitive, confidential or classified data
- Ensure hard drives from machines no longer in service are removed and stored securely in a locked premise or wiped clean
- Ensure any 'smart device' such as an iPad are secured with a start-up pin. Many such devices have access to contact information and confidential emails thus creating a significant security risk.
- Never save confidential or sensitive data locally to a school mobile device, such as a laptop or iPad.
- Administration staff must never have sensitive information on the main reception desk at any time. The only information that is acceptable is student forename, surname, DOB and year\form data. All other data is excluded in paper format. This includes but is not limited to:
- Printing letters to parents
- Working on student examination entry forms
- Opening confidential student medical information

Remote Access - VPN

- You are responsible for all activity via the school's VPN 'Redhill School'
- All activity through the school's VPN is logged and can have reports generated to record activity as and when requested.
- Only use equipment with an appropriate level of security for remote access.
- To prevent unauthorised access to school systems, keep all dial-up access information such as logon IDs and PINs confidential and do not disclose them to anyone

- Redhill's VPN is only permitted for Redhill staff. Access is controlled and monitored by the IT team. Access can be revoked when required.
- Only RoarTech and Redhill IT have administrative access to the school VPN. This included additional security via the implementation of L2TP/IPSEC with a PSK on top of a user/password combination to enhance our VPNs security.

- If a device happens to be reported lost or stolen, membership will be revoked by disabling VPN access and machines Active Directory account.
- Do not write down or otherwise record any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it pertains to
- Protect school information and data at all times, including any printed material produced while using the remote access facility

Senso

The school has purchased Senso software for Classroom and Student Safety. Senso monitors all users IT interactions, across PC's and laptops, from key words typed, images searched, Team group chats, all applications opened, websites visited and more. All logs are stored centrally for viewing\processing\actioning or flagging as false positive. Any reports are passed to the headteacher for investigating.

Policy - Records for off site working

To plan, record, assess and effectively deliver learning and development requires various paper and electronic documents. At times it is necessary and appropriate for staff to take these resources off site. At times school staff may be required to attend meetings off site to discuss pupils and sometimes staff. Records may need to be transported to and from those meetings.
These records may include personal data and particularly sensitive data. Ensuring that data is properly cared for and managed whilst off site is an obligation for the school and the individual who is removing the data.

Procedure

Any records that are removed from site need to be identified. More sensitive information will require specific permission, either on a case by case basis or as part of that member of staff's role and responsibilities
The records may include (but is not limited to):

- Lesson Planning
- Marking
- Attendance spreadsheet
- Cohort tracking document
- Letters to parents
- Electronic document containing parent/carer information
- Safeguarding information
- Staff contact details
- Staff appraisals, observation and supervision records
- SEND records
- Accounting and invoice information and documents
- School finance information

All laptops and tablets within the setting are **encrypted** and are anti-virus protected and are locked away when not in use.

Records and data may only be stored at home i.e. not to be left in a car or car boot or anywhere that they can get lost or misplaced i.e away from family members and visitors and not shared with others under any circumstances and **MUST** be stored away securely when not in use preferably in an office or a lockable bag or case.

Any loss, theft or sharing of that data must be reported at the earliest opportunity to consider if there has been a data breach. Early reporting can enable efficient management of the risks.

Any member of staff that uses the information that is taken home for anything other than the intended purpose will be managed using the disciplinary procedures and reported to Local authority designated officer (LADO) and the Information Commissioner's Office (ICO).

Filtering and monitoring standards – responsibilities of all school staff

A safe online environment is essential for teaching and learning. Therefore, the filtering and monitoring standards in place are important in order to safeguard staff and students from harmful or inappropriate content.
In line with the first standard, system management, see below our key personnel
The lead individual within the Senior Leadership Team, is Amy Coughlan, who you should contact with any queries relating to this topic.
In line with the safeguarding policy, any safeguarding concern should be immediately directed to the Designated Safeguarding Lead (DSL), Claire Whiting
If you have queries regarding the implementation of the monitoring and filtering systems, please discuss this with our IT lead, Rich Robey or Lawrence Whiting.
All staff in the school have the following responsibilities to ensure the standards are effectively implemented.

You must:

- know how to report and record any concern where you have witnessed or suspect harmful content has been accessed.
- approach your IT lead if you are unsure whether the filtering system is working successfully on your school device.
- inform the SLT and IT lead if you can access unsuitable material.
- notify the named leads if you are teaching topics which may create unusual activity or alerts.
- discuss any unreasonable restrictions that affect teaching, learning or administrative tasks with your named leads.
- promptly report failure or abuse of the system.
- report any abbreviations or misspellings that allow access to restricted material.
- provide effective supervision of students when using school devices.
- maintain awareness of how devices are being used by students.
- be aware of the online safety, acceptable use and safeguarding policies.

Signed: ……..

Print Name: ……..

Date: ……..