



Education Trust

Inspiring the individuals of today, for a better society tomorrow,
“Aspire, Belong, Collaborate”

INFORMATION SECURITY POLICY incorporating TECHNICAL SECURITY POLICY

Review Frequency	Annual
Reviewed	3.11.2025
Next Review	November 2026
Agreed by Trustees	5 th December 2025

Contents

INTRODUCTION 3

ROLES & RESPONSIBILITIES 4

AREAS THAT REQUIRE SPECIFIC ADOPTION OF INFORMATION SECURITY 7

ASSOCIATED POLICY & GUIDANCE 11

 Introduction 12

 Responsibilities 12

TECHNICAL SECURITY 12

 Policy statements 12

PASSWORD SECURITY 14

 Policy Statements: 14

 Password requirements 14

 Learner passwords: 15

 Protocols for the RET technical staff team 15

 Training/Awareness: 16

FILTERING 16

 Responsibilities 16

 Policy Statements 17

 Education/Training/Awareness 18

 Changes to the Filtering System 18

 Monitoring 18

 Audit/Reporting 18

 Further Guidance 18

 Details of Amendments20

INTRODUCTION

The Riviera Education Trust is responsible for the control of a number of individuals' Personal Data (including staff, governors, pupils, clients, and a number of other individuals who interact with Riviera Education Trust). In addition to personal data, information that may be considered of a sensitive nature will include financial records, planning and management forecasts, and risk assessments, which also require appropriate security applications to be made and are included within the scope of this policy.

The Information Security Policy is designed to inform employees of the appropriate principles and methods to create, store, secure and dispose of information in all formats to ensure security is of a consistently high standard. Compliance with this Policy provides management, staff and associated individuals with:

- Assurance that information is being managed securely in a consistent and effective way.
- Assurance that Riviera Education Trust is able to provide a trusted environment in which to handle information as part of its activities.
- Clarity regarding the individual responsibilities for Information Security.
- Demonstration of best practice.
- Assurance that information may only be accessed by those authorised to have access.

SCOPE

This policy applies to all employees of the Riviera Education Trust including contract, agency and temporary staff, volunteers and employees of partner organisations working with or for the Riviera Education Trust.

This policy can be used by employees who use data as part of their day-to-day business, those who manage and administer data and by those responsible for the management of data storage systems.

AIM

The Information Security Policy aims to ensure that all employees are aware of the following principles of the CIA Triad (Confidentiality, Integrity and Availability) when dealing with information and use the principles from their day-to-day handling of information up to the development and adoption of new ways and systems designed for handling information. These principles will also help the Riviera Education Trust comply with Article 32 of the GDPR which refers to adequate organisational and technical security;

Confidentiality

Information is not made available or disclosed to unauthorised individuals, entities, or processes.

Integrity

Maintain the accuracy and completeness of data over its lifecycle.

Availability

Information must be available when needed and appropriate means of access or disclosure must be understood.

In addition to the protection and maintenance of the confidentiality, integrity, and access of data this policy will support the Riviera Education Trust to meet the following:

- manage the risk of security exposure or compromise;
- assure a secure and stable information technology (IT) environment;
- identify and respond to events involving information asset misuse, loss or unauthorised disclosure;
- monitor systems for anomalies that might indicate compromise; and
- promote and increase the awareness of information security.

Adoption of this concept will reduce the risk of harm to individuals, reduce the vulnerability of the organisation and the likelihood of financial penalties that may be given by supervisory authorities such as the Information Commissioner's Office (ICO).

ROLES & RESPONSIBILITIES

Information Security Lead

Accountability for Information Security rests with the Information Security Lead who is the CEO. The Information Security Lead may discharge this function to the Head of School, Data Protection Lead or another responsible individual to carry out the activities of Information Security.

Such activities may include.

- Evaluating and accepting risk on behalf of the school.

- Identifying information security responsibilities and goals and integrating them into relevant processes.
- Supporting the consistent implementation of information security related policies and processes.
- Supporting security through clear direction and demonstrated commitment of appropriate resources.
- Promoting awareness of information security best practices through the regular dissemination of relevant material such as that provided by the Data Protection Officer (DPO).
- Implementing the process for determining information classification and categorisation, based on recommended practices, and legal and regulatory requirements, and to determine the appropriate levels of protection for that information.
- Implementing the process for information asset identification and recording them in the Record of Processing Activities (RoPA) as well as the handling, use, transmission, and disposal based on information classification and categorisation.
- Determining who will be assigned to serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data.
- Participating in the response to security incidents.
- Complying with notification requirements in the event of a breach of personal data.
- Adhering to specific legal and regulatory requirements related to information security.
- Communicating legal and regulatory requirements to the designated security representative (e.g. Information Security Officer ISO), specifically article 32 of the UK GDPR (security of processing).
- Communicating requirements of this policy and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements.
- Development of localised guidelines for the use of specific systems, training plans, threat awareness and updates, spot checking and auditing.

Governance of Information Security may be formalised to include a regular review and working group to identify business requirements and how they impact existing information use and future use.

Data Protection Officer (DPO)

The DPO, Data Protection Education, is responsible for monitoring the organisation's compliance with Data Protection legislation. This is completed by the following means: an annual assurance review;

breach and security incident monitoring; and review and providing sufficient guidance to the Information Security Lead for them to carry out their task where personal data may be processed.

The DPO will support the organisation in the event of any breach of information where it relates to personal data.

Heads of School / Team Leads

Heads of School / Team Leads are primarily responsible for ensuring the security of their physical environments where information is processed or stored. They are also responsible for the following:

- Ensuring all employees within their area of work are aware of the relevant policies applicable to their role i.e. Acceptable Use Policy, Confidentiality agreements, Bring Your Own Device Guidelines and eSafety Guidelines
- Determining and controlling the access levels of employees and relaying that information, including when access must be removed, to the IT Team.
- The control of passwords, keys, combination lock numbers or any other physical form of access control within their area of work.
- Ensuring that employees have taken part in the relevant and adequate training in a timely manner.
- Making employees aware of security breaches or threats and translating points learnt from such incidents into working practices.

IT Team

The IT Team whether on-site or through a third-party contract must ensure that all network, Trust devices and any removable media assets are securely controlled and managed. This includes maintaining appropriate storage facilities, producing and reviewing guidance regarding the safe storage and use of assets, user access agreements and user access control, such as the removal of users when informed to do so by managers, or under exceptional circumstances.

The maintenance of software in use by the organisation. This includes software patching routines, application or alterations or the removal of software considered to be vulnerable, the assessment of such levels of vulnerability, and the notification to all relevant staff of existing threats, emergent threats, and appropriate safe use. This information may be provided to managers in support of their responsibilities for awareness.

The development and implementation of new technologies to build safe and secure systems. The direction of this responsibility should be agreed with the Information Security Lead.

Information Owners/Responsible Persons

The approach to the use of data will determine who Information Owners are. In general, the ownership or responsibility will fall to the relevant manager, or person who retains and uses the information within their workspace, for example the Lead Administrator will own the data used within the academy offices, including centralised pupil information; the Designated Safeguarding Lead (DSL) will own Safeguarding Information; and individual teachers will own class lists and pupil information where it is not held on the Pupil Information Management System.

It is good practice to record the relevant owner or responsible person so that any issue regarding the use, management or breaches of that information may be brought to their and the DPO's attention. This is referred to as an Information Asset List, however it may be incorporated into the Record of Processing Activities used for Data Protection purposes.

Information Owners will be responsible for managing the accuracy and security of their data. This will mean that their relationship with their peers and managers, where applicable, is key to ensuring the CIA Triad is observed. Owners will also need to discuss with the Information Security Lead and DPO the implications of using third parties to process information or when sharing information. Where this includes personal data or other sensitive information, appropriate agreements must be in place.

All Employees and External Individuals

Everyone is responsible for Information Security and should be aware of and understand the requirements of them in line with this Policy and any associated guidance, such as Online Safety, Acceptable Use, confidentiality agreements and the conditions of use of any device issued by the Riviera Education Trust.

The key points for all employees to remember are;

- What information they are using, and how it should be handled, stored, or destroyed.
- What procedures, standards and agreements exist for the sharing of information with others.
- How to report breaches.
- Their responsibility for raising their concerns with their manager, the relevant Information Owner, DPO or Information Security Lead.

- In the event that RET staff or Governors use their personal phone to access their school email or google drive, they must ensure that their device is updated and securely password protected.

Individuals who may work in the Trust with information but not be an employee, such as IT consultants, auditors or external agencies, should be able to demonstrate their organisation's Information Security approach or have an appropriate confidentiality statement within their work description.

They should be made aware of what they should do if they inadvertently access information that they should not have done or discover a breach. This may be as simple as letting them know to contact the person who is responsible for them or making them aware of who the relevant manager is that they can report to.

AREAS THAT REQUIRE SPECIFIC ADOPTION OF INFORMATION SECURITY

Contracts of Employment

Staff suitability must be assessed at all points of employment, in line with safer recruitment policies and guidance, and all employee contracts must contain reference to confidentiality. Information in the form of the Acceptable Use Policy, Data Protection Policy or specific confidentiality guidance must be provided to employees at the appropriate time.

Control of Information Access

Information shall be restricted to only those who have an acceptable business reason to access such information. Information Owners/Responsible Persons must be consulted before access is granted or an appropriate process of access must be in place. Passwords or emergency access without authorisation may only be made in exceptional circumstances and the decision to do so must be relayed to the relevant Information Owner, Manager, or the Information Security Lead at the earliest possible point.

Staff Owned Devices - Bring Your Own Device (BYOD)

- Staff must not use their own devices to take images of young people. Only Trust equipment may be used, and images must be deleted as soon as they are no longer required, saved securely on the Trust Google Drive, and deleted in accordance with the retention policy

- Pass-codes or PINs must be set on personal devices to aid security and where possible, encryption applied to the device.
- Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements.
- Users must log out of Trust programmes and applications when they are not in use.
- The device must have the latest updates applied
- Passwords must not be saved, for example to the browser history.
- Users must not download data locally to the device (e.g. email attachments).

Computer Access Controls

Access to computer systems must be managed by the IT Team. This may be by active directory or, in the case of portable devices, by providing a temporary password. There must be a form of system monitoring that can be used to determine who accessed which device and at what time, at a basic level this may be using Active Directory, Event Viewer or a more complex User activity Monitor (UAM) software. The fundamentals of password security are required to ensure that passwords are not shared which would result in misidentification with the exception of the point regarding emergency access in the previous paragraph.

Application Access Controls

Specific applications must be administered effectively by either IT or the responsible person for any third-party application, such as Seesaw. This is particularly relevant for the Pupil Management System, however applies to all other applications where it has been deemed that access controls are required. When adopting a new application, a proper assessment of access controls must be made and, if necessary, locally produced guidelines regarding its use should be made. This may be covered as part of a Data Protection Impact Assessment.

Equipment Security

Information may be stored in physical containers such as filing cabinets, drawers, safes and storage rooms. It will in most cases be retained electronically, however the principles of security are the same.

Any area where information is stored must be secured in a manner appropriate to the type and sensitivity of information stored within, for example sensitive financial records, safeguarding records and HR records must be secured by lock, or if stored electronically on a secure cloud or section of the computer network isolated by specific permissions. General lists and necessary contact details should be stored out of sight in line with a clear desk routine, or, if stored electronically, may be stored in a

general open section of the computer network. Information Owners must make an assessment of the level of security required and where necessary consult with the Information Security Lead and IT Team. In cases where highly sensitive information is stored electronically, it should be encrypted wherever possible.

Computer Network Procedures

The arrangement and control of the computer network should be documented and must not remain with a single person. The reliance upon a sole individual's understanding of the system can undermine the principle of availability, if they leave or are unavailable, due to the potential loss of access, and may lead to loss of data if a full understanding of the type and location of data is not retained.

Information Security Breaches and Reporting

Any breaches of information security must be reported to the Information Security Lead and, where it involves the inappropriate access via hacking, malicious attack, lack of security around an electronic system, loss of physical device or any other similar situation, IT must also be informed.

In instances where there is the potential breach of personal data the DPO must also be informed at the earliest possible point.

The confidentiality or security of information that has been breached which was held in a physical format, i.e. paper record, application form or folder, does not need to be reported to IT in most circumstances, however the Information Security Lead must still be informed.

Protection from Malicious Software

Riviera Education Trust and its IT providers shall use software protection to detect and deny intrusion, email filtering and if possible, adopt measures such as SPF, DKIM and DMARC (to stop the organisation's email addresses getting spoofed). Users are not to install software on the Organisation's network without prior approval or introduce malicious software via other routes, i.e. the use of unmanaged USB devices.

The IT Team should have a documented process for Cyber Security, seek formal accreditation of IT processes, or adopt standards that equate to accreditation.

Removable Media

Any removable media should not be needed to be used, as the Google Drive supports secure file transfers, other than SD cards for cameras which should be safely managed by the staff user.

Any external information device that someone wishes to use should be submitted to their manager and IT for approval prior to use. Where personal data or information of a sensitive nature may be stored, encryption must be applied to the device.

Monitoring System Access and Use

Systems should, where possible, be adopted that can provide an auditable trail of access, this is considerably more important as the type and sensitivity of the information being accessed increases. In terms of physical records, this may be limited to a single or small number of individuals or a signing in and out form, this may be particularly applicable to records that contain special categories of personal data.

Electronic systems will, in many cases, have event record logs, however the Organisation must ensure that they understand how this function works and how it may be used when required, or, if it is inadequate, be able to work with the IT Team or IT provider to apply any additional software as necessary.

The Trust must make it clear to employees that information contained on the Organisation's system is subject to access and monitoring and that, except in exceptional or agreed circumstances, should not be used for personal reasons by employees. The limitations of this are defined in the Acceptable Use Policy, contract terms or specific guidelines created for this purpose.

Accreditation and Assessment of Systems

The Information Security Lead must be assured that new systems, be they physical or electronic, are adequately assessed by the relevant manager, IT Team or responsible person. Such assessment may not need to be formally documented but demonstration of the assessment must be recorded appropriately. Recognised accreditation will provide a significant level of assurance; however, it must be taken into account with the intended way of using any application.

System Control Change

Any change made to any system must be confirmed with the Information Owners and, where any conflict arises, must be referred to the Information Security Lead. Access abilities to alter any system parameters should adhere to the Principle of Least Privilege.

Business Continuity and Disaster Recovery Plans

The Information Security Lead is responsible for ensuring that, in the event of any catastrophic failure of a system, there is adequate capability for the continuation of the use of information in line with the CIA Triad. Any system which is deemed to be critical to the organisation should be included within a Business Continuity Plan, this may include the Pupil Management System, access to financial resources or safeguarding information.

Training and Awareness

Information security may not be considered a separate training topic in its own right; however, the CIA Triad should underpin any training in relation to the processing of data. This will include system use and operation, data protection training, safeguarding, and procurement training.

ASSOCIATED POLICY & GUIDANCE

RET Data Protection Policy
RET Acceptable Use Policy
RET Technical Security Policy incorporated in this policy
RET Online Safety Policy

TECHNICAL SECURITY POLICY

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The Riviera Education Trust will be responsible for ensuring that Riviera schools' IT infrastructure and networks are as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes or collaborative working within the RET policies)
- access to personal data is securely controlled in line with the RET GDPR data protection policies
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have an impact on policy and practice

Responsibilities

The management of technical security will be the responsibility of the Riviera Education Trust ICT Team and the SLT Digital Lead.

TECHNICAL SECURITY

Policy statements

The Riviera Education Trust will be responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- Riviera Education Trust technical systems will be managed in ways that ensure that the Riviera Education Trust meets recommended technical requirements.
- there will be regular reviews and audits of the safety and security of the Riviera Education Trust's technical systems.
- servers, wireless systems and cabling must be securely located and physical access restricted.
- appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school/Trust systems and data.
- responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff

- all users will have clearly defined access rights to the Trust technical systems. Details of the access rights available to groups of users will be recorded by the Riviera Education Trust IT Team and will be reviewed, at least annually, by the SLT Digital Lead.
- users will be made responsible for the security of their username and password, and they must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security (*see password section below*).
- the Riviera Education Trust IT Team is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- mobile device security and management procedures are in place for school owned mobile devices. These are a combination of Apple School Manager, Jamf, Meraki and G Suite Admin Console.
- the Riviera Education Trust technical staff regularly monitor and record the activity of users on the Trust schools technical systems and users are made aware of this in the acceptable use agreement. This monitoring is done through Senso and RM Safetynet reporting systems as well as mobile device management systems.
- remote management tools can be used by staff to control workstations and view pupil's activity.
- an appropriate system is in place for users to report any actual/potential technical incident to the school's online safety subject leader/Riviera Education Trust IT Team. These reports are made by logging a helpdesk call on the Riviera Education Trust Helpdesk or phoning directly for urgent incidents.
- an agreed policy is in place for the provision of temporary access of 'guests', (e.g. trainee teachers, supply teachers, visitors) onto the Trust system. Guests may be given a temporary named login where applicable for their use on the system. They are made aware of this policy and must agree to the relevant policies prior to use of the accounts. Once the guest access is no longer required, accounts are suspended/deleted from the system.
- an agreed policy is in place regarding the downloading of executable files and the installation of programs on Riviera Education Trust devices by users. Executable files should only be downloaded and installed on Riviera Education Trust Devices with prior permission from a member of the Riviera Education Trust IT Team.
- an agreed policy is in place regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on Trust devices that may be used out of school. Users may use, with prior permission, devices owned by the Trust for their own personal use as long as there is no detrimental effect to the device or security itself. Users must also be aware that their device can be requested by a member of the Riviera Education Trust IT Team at any time and they agree to unlock any device that they have locked with their own account for any member of the IT Team.
- an agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on Trust devices. Removable memory sticks are not generally used with computers

within the Riviera Education Trust as the secure Google Drive has replaced these. For files that require transfer onto devices, a Riviera Education Trust Google account should be used to transfer items to the device. SD cards for transferring photographs/videos from cameras to computers can be used but they must only be used for this purpose. See Online Safety Policy.

- the Riviera Education Trust infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc.
- personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

PASSWORD SECURITY

A safe and secure username/password system is essential if the above is to be established and will apply to all the Riviera Education Trust technical systems, including networks, devices, email and learning platforms.

The Riviera Education Trust provides G Suite for Education logins to all employees throughout the Trust. Two factor authentication must be enabled on these accounts and authenticated with either a U2F mobile key or by another method for all members of staff accounts.

Further guidance can be found from the [National Cyber Security Centre](#) and [SWGfL "Why password security is important"](#)

Policy Statements:

- These statements apply to all users
- All Trust networks and systems will be protected by secure passwords
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Riviera Education Trust IT Team and will be reviewed, at least annually, by the online safety group
- All users (adults and pupils) have responsibility for the security of their username and password, must not allow other users to access the systems using their logon details and must immediately report any suspicion or evidence that there has been a breach of security
- Passwords must not be shared with anyone
- All users will be provided with a username and password by the Riviera Education Trust IT Team who will keep an up-to-date record of users and their usernames

Password requirements

- Passwords should be at least 8 characters long and include upper case letters, lower case letters, numbers and punctuation
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school

- Passwords must not include names or any other personal information about the user that might be known by others
- Passwords must be changed on first login to the system
- 2 factor authentication is enforced for all staff G Suite accounts and it is highly recommended for any other account linked to the Trust where this option is available
- Passwords should be changed regularly as part of the cyber security cycle

Learner passwords:

- All pupils should have unique passwords for logging in to G Suite accounts as well as other accounts for online platforms.
- Pupils should not share their passwords with other pupils and should not log in to any account belonging to any other pupils.
- Whole class logons must not be used for access to online programs due to not being able to identify any individuals who may have infringed the rules set out in this policy and the Acceptable User Agreement.
- Pupils will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Protocols for the RET technical staff team

- Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level. 2 Factor Authentication for these accounts, where available, must be used.
- An administrator account password for the Trust systems should also be kept in a secure place e.g. Trust/School safe. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account.
- Users should be able to set their own passwords on account creation either through a reset link or by being asked to change their password on first login. Where possible a reset link should be sent and a generic first password should not be set on the system.
- Requests for password changes should be authenticated by the account user or by a member of SLT to ensure that the new password can only be passed to the genuine user.
- Requests for new user accounts should be made/authorised by either the Head of School, HR team or the CEO of the Riviera Education Trust before being created by the IT Team. These requests should be logged on the helpdesk by the member of staff with the authority to request accounts.
- Suitable arrangements should be in place to provide visitors with appropriate access to systems which expire after use.
- In good practice, the account is 'locked out' following six successive incorrect log-on attempts.
- Passwords shall not be displayed on screen, and shall be securely hashed when stored (use of one-way encryption).

Training and Awareness:

It is essential that users should be made aware of the need for keeping passwords secure and the risks attached to unauthorised access/data loss. This should apply to even the youngest of users. It is also essential that users be taught how passwords are compromised, so they understand why things should be done a certain way.

Members of staff will be made aware of the Trust's policies on passwords:

- at induction
- through the RET online safety policy
- through the acceptable use agreement

Audit/Monitoring/Reporting/Review:

The Riviera Education Trust IT Team will ensure that full records are kept of:

- User ids and requests for password changes
- User logons
- Security incidents related to this policy

FILTERING

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. We recognise the importance that the Trust has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in school. DfE Keeping Learners Safe in Education requires schools to have appropriate filtering. Riviera Education Trust adheres to guidance from the UK Safer Internet Centre site.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Riviera Education Trust ICT Team/Online Safety Lead. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must (schools should choose their relevant responses):

- be logged in change control logs
- be reported to a second responsible person
- be reported to and authorised by a second responsible person prior to changes being made (recommended)

- be reported to the SLT Digital Lead every term; in the form of an audit of the change control logs

All users have a responsibility to report immediately to the Riviera Education Trust ICT Team/SLT Digital Lead any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programs or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school maintains and supports the managed filtering service provided by the Internet Service Provider RM
- Members of Staff have different access to pupils so they can access sites which may be required for education but are not suitable for pupils, e.g. Youtube
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head of school.
- Mobile devices that access the school internet connection (whether Trust or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately by the technical team to the filtering provider, RM.
- Requests from staff for sites to be removed from the filtered list will be considered by the Riviera Education Trust IT Team/SLT Digital Lead. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.

Education, Training and Awareness

Pupils will be made aware of the importance of filtering systems through the online safety education curriculum. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the acceptable use agreement
- induction training
- staff meetings, briefings, INSET.

Parents will be informed of the school's filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletters/alerts.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to The Riviera Education Trust IT Team/SLT Digital Lead by emailing itsupport@rivieraet.co.uk.

This request will then be passed to the Head of School for their approval. Once approved/rejected by the Head of School, appropriate action will be taken by the IT Team to filter/unfilter any site requested.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the school online safety policy and the acceptable use agreement. Monitoring will take place using the Senso online program which sends live alerts directly to DSLs and Heads of School for any high priority safeguarding content.

Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- The Riviera Education Trust IT Team/SLT Digital Lead
- Online Safety Governor/Governors committee
- RM/Local Authority/Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision. (The evidence might show a large number of requests to remove the filtering from sites – in which case schools might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring/disciplinary action might be necessary).

Further Guidance

Schools in England (and Wales) are required *“to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering”* (Revised Prevent Duty Guidance: for England and Wales, 2015).

SWGfL provides a site for schools to test their filtering to ensure that illegal materials cannot be accessed: [SWGfL Test Filtering](#)

DETAILS OF AMENDMENTS

November 2020

- New policy from DPO iWest

27.1.22

- Passwords should be changed regularly as part of the cyber security cycle.
- Managed Filtering Service is provided by RM

April 2023

- Reviewed without change.

7.10.24

- Added Data Protection Lead to Information Security Lead function list
- Monitoring - Monitoring will take place using the Senso online program which sends live alerts directly to DSLs and Heads of School for any high priority safeguarding content.
- Filtering - updated to remove the staff proxy as now managed by User Based Filtering

3.11.25

- Updated Roles and Responsibilities to add reference to Bring Your Own Device Policy
- Updated Areas that require specific adoption of information security to include “Staff Owned Devices - Bring Your Own Device (BYOD)” section

6/5/26

- Details added of new DPO, Data Protection Education (from 25/5/26)