Staff IT Acceptable Use Policy

Person responsible for policy: IT Technical Director

Revised: October 2019

Next Review Date: October 2020

Summary and Key Points

All Staff, Governors and anyone else who has been given approved access to use RLT systems must read this summary and the entire document and then print, sign and complete the declaration on the last page, before passing back to your HR Officer for retention on your staff file.

This Acceptable Usage Policy covers the security and use of all River Learning Trust or member schools (hereafter called RLT Schools) information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment and applies to all River Learning Trust or member school (RLT Schools) employees, contractors and agents (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form, relating to RLT Schools activities, and to all information handled by RLT Schools relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by RLT Schools or on its behalf.

Individuals must not:

- Allow anyone else to use their user ID and password on any RLT Schools IT system. Any compromise must be reported to IT Support and you must change your password.
- Leave their user accounts logged in at an unattended and unlocked computer, or use someone else's User ID or password to access systems.
- Perform any unauthorised changes to or access RLT Schools IT systems or information, including disabling, removing or installing any software without authorisation from IT Support including anti-virus software.
- Connect any unauthorised device to the RLT Schools network or IT systems without the express consent of the school IT Support and only in accordance with this policy. Similarly, authorised RLT Schools items must not be disconnected.
- Store RLT Schools data on any non-authorised RLT Schools equipment; e.g. mobile phones, digital cameras, memory or flash sticks. Personal devices **must not** be used for creating, recording or transferring images of children and young people.
- Give or transfer RLT Schools data or software to any person or organisation outside RLT, or place any such information on the internet.
- Send unprotected (ie not password protected or encrypted) sensitive or confidential information externally or via email.
- Forward RLT Schools mail to personal (non RLT Schools) email accounts (for example a personal email account).
- Use the internet or email for the purposes of harassment or abuse, or which may affect its reliability or effectiveness or which contain profanity, obscenities, or derogatory or discriminatory remarks including (but not limited to) those concerning sex, sexual orientation, age, race, religion, gender or disability in communications, or which may bring RLT Schools, into disrepute. Similarly, not download or access any such information or data.
- Open or download any emails or attachments from unknown sources without carefully considering their integrity, if there is any doubt contact IT Support for guidance.
- Use the internet or email to make personal gains or conduct a personal business, gamble or take part in on-line auctions.
- Make official commitments through the internet or email on behalf of RLT Schools unless authorised to do so.

- Download any file or data which in any way infringe any copyright, database rights, trademarks or other intellectual property copyrighted material such as (but not limited) to music media files, photo and video files and text, without appropriate approval.
- Download any software from the internet without prior approval of the IT Department.
- Connect RLT Schools devices to the internet using non-standard connections.
- Store personal files such as music, video, photographs or games on RLT Schools IT equipment.
- Use RLT Schools voice equipment for conducting private business.
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or International operators, unless it is for business use.
- Accept Social Media invitations from children and young people to 'add me' (or equivalent) as a friend to their social networking sites, nor will individuals invite children and young people to be 'friends' on theirs.

Individuals need to ensure:

- Computers must be logged off/locked or protected with a screen locking controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers, photocopiers and desks.
- All 'business'-related confidential printed matter must be disposed of using confidential waste bins or shredders.
- All critical documents (including anything with personal data) are held in Google Drive or a backed up network drive rather than the devices local storage. 'Downloads' folders are not usually network drives.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a vehicle.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption **must** be used.
- If your computer equipment is lost or stolen you must report the incident to IT Support and to the Site Manager immediately, and notify your line manager as soon as possible.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption. Laptops must be protected through an encryption method such as Bitlocker.
- It is strongly recommended that all online accounts are protected by two factor authentication.
- That any private social networking sites / blogs etc. that they create or actively contribute to, are not confused with their professional role in any way, or the opinions and position of RLT Schools.
- RLT Schools telephone equipment (including mobile telephony) is intended for business use only.
- Where a video conference facility including that over the web (such as Skype of Hangouts etc) or web chat facilities are used, these must be for RLT Schools purposes only.

Policy and Guidance

Computer Access Control

Access to the RLT Schools IT systems is controlled by the use of User IDs, passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the RLT Schools IT systems.

Individuals must not:

- Allow anyone else to use their user ID and password on any RLT Schools IT system. If there is any suspicion or doubt that an individual's password has been compromised then the individual must change it immediately and contact the schools IT Support.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access RLT Schools IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to RLT Schools IT systems or information.
- Access of attempt to access data that they are not authorised to use or access for the performance of the duties of their role.
- Exceed the limits of their authorisation or specific 'business' need to interrogate the system or data.
- Connect any non RLT Schools authorised device to the RLT Schools network or IT systems without the express consent of the school IT Support and only in accordance with this policy. Similarly authorised RLT Schools items must not be disconnected.
- Use personal devices be used for creating, recording or transferring images of children and young people.
- Give or transfer RLT Schools data or software to any person or organisation outside RLT Schools without the authority of a member of the Senior Leadership Team at their school or a senior member of the RLT Central Team

Individuals must make sure that

- Where private devices are used to access an RLT G Suite, users are responsible for reporting loss or theft of such devices to IT Support. IT Support will then revoke sign-in rights and remotely wipe the device. Be aware that a degree of device management will be silently installed on any device an RLT account is used on. **Only RLT accounts** should be used for creating, recording or transferring images of children and young people.
- all critical documents (including anything with personal data) are stored on Google Drive or a network drive rather than the PCs/laptop's hard drive. 'Downloads' folders are not usually network drives.
- If your computer equipment is lost or stolen you must report the incident to IT Support and to the Site Manager immediately, and notify your line manager as soon as possible. The incident will be fully investigated, and may be treated as a disciplinary issue if you have failed to take adequate steps to safeguard the security of equipment in your possession.

Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

Internet and email Conditions of Use

Use of RLT Schools internet and email is intended for 'business' use. Personal use is permitted where such use does not affect the individuals 'business' performance, is not detrimental to RLT Schools in any way, nor in breach of any term and condition of employment and does not place the individual or RLT Schools in breach of statutory or other legal obligations. Any personal use must be in the individuals own time.

Individuals must not visit, or attempt to visit, websites that might be considered inappropriate or illegal. Staff need to be aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use or send in attachments profanity, obscenities, or derogatory or discriminatory remarks including (but not limited to) those concerning sex, sexual orientation, age, race, religion, gender or disability in communications, or which may bring RLT Schools, into disrepute.
- Access, download, send or receive any data (including images), which may be considered offensive in any way, including but not limited to, sexually explicit, discriminatory, defamatory or libelous material, or that which does not uphold fundamental British values. Inform your manager straight away if you accidentally access an illicit/inappropriate website
- Open or download any emails or attachments from unknown sources without carefully considering their integrity, if there is any doubt contact IT Support for guidance.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble or take part in on-line auctions.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to RLT Schools, alter any information about it, or express any opinion about RLT Schools, unless they are specifically authorised to do so.
- Send unprotected (ie not password protected or encrypted) sensitive or confidential information externally or via email.
- Forward RLT Schools mail to personal (non RLT Schools) email accounts (for example a personal email account).
- Make official commitments through the internet or email on behalf of RLT Schools unless authorised to do so.
- Download copyrighted material such as (but not limited) to music media files, photo and video files and text, without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the IT Department.
- Connect RLT Schools devices to the internet using non-standard connections.
- It is strongly recommended that all online accounts are protected by two factor authentication.

Email and other electronic communication with students **must only** be carried out through school systems. Individuals must not give any personal contact details to students. (E.g. private email address, mobile phone number). There is a school Mobile available to take on trips

Social Media

Social Media plays a significant role in today's society, but it is important that all staff take particular care when accessing as using sites such as Facebook, Twitter or other similar sites and apps.

- **Individuals must not** accept invitations from children and young people to 'add me' (or equivalent) as a friend to their social networking sites, nor will individuals invite children and young people to be 'friends' on theirs, damage to professional reputations can inadvertently be caused by quite innocent postings or images. Individuals also be careful with who has access to their pages through friends and friends of friends. Especially with those connected with their professional duties, such a school parents and their children.
- **Individuals need to ensure** that any private social networking sites / blogs etc. that they create or actively contribute to, are not confused with their professional role in any way, or the opinions and position of RLT Schools

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, RLT Schools enforce a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided, for example secure print on printers.
- Computers must be logged off/locked or protected with a screen locking controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers, photocopiers and desks.
- All 'business'-related confidential printed matter must be disposed of using confidential waste bins or shredders.

Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- when working from school, home or other location. Work carried out must always be with due regard to the terms of this policy and to data protection/confidentiality issues.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption. Laptops must be protected through an encryption method such as Bitlocker.

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs, removable hard drives and phones must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only RLT Schools authorised mobile storage devices with encryption enabled must be used when transferring sensitive or confidential data.

Employees must use only software that is authorised by RLT Schools (or the respective schools IT Department) on RLT Schools computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on RLT Schools computers must be approved and installed by the RLT Schools IT department.

Individuals must not:

- Store personal files such as music, video, photographs or games on RLT Schools IT equipment.
- Remove or install any software without authorisation from IT Support.

Viruses

The IT department has implemented centralised, automated virus detection and virus software updates within the RLT Schools. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved RLT Schools anti-virus software and procedures.

Telephony (Voice) Equipment and Video and web conferencing and chat facilities.

Use of RLT Schools telephone equipment (including mobile telephony) is intended for business use only. Individuals must not use RLT Schools voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications.

Individuals must not:

- Use RLT Schools voice for conducting private business.
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or International operators, unless it is for business use.

Where a video conference facility including that over the web (such as Skype of Hangouts etc) or web chat facilities are used, these must be for RLT Schools purposes only. As such individuals must ensure that access is not provided (both via data access and video or chat) of any item or subject which might be considered confidential to RLT Schools. Special care should be taken to see what is visible in any video chat eg. images and names of students or even the individuals own family. Chats of this nature can become less formal so care should also be taken to ensure that the RLT Schools professional standards and expectations are maintained at all times.

Actions upon Termination of Employment or Contract

All RLT Schools equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to RLT Schools on termination of employment or contract

All RLT Schools' data or intellectual property developed or gained during the period of employment remains the property of RLT Schools and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering

All data that is created and stored on RLT Schools computers is the property of RLT Schools and there is no official provision for individual data privacy. However wherever possible RLT Schools will avoid opening personal emails, if these can be easily and clearly identified as such. Systems may be accessed at the Headteacher's discretion during an individual's absence to ensure continuation of education and the functioning of RLT schools

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. RLT Schools has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 2018, the Computer Misuse Act 1990, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000. This policy should be read in conjunction with these pieces of legislation

It is your responsibility to report suspected breaches (including by others) of security policy without delay to your line management and the IT department. All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with RLT Schools disciplinary procedures. You may use Raising Concerns at Work or Whistleblowing Policies to report such incidents.

Confidentiality
Individuals must not use the school's ICT and communications systems whether alone or in conjunction with any other device to make an unauthorised disclosure or copy of confidential information belonging to the school.

The unauthorised disclosure or copying of information belonging to the school is likely to be treated as a disciplinary offence and could give rise to a dismissal for gross misconduct

Such confidential information shall include without limitation details of staff contact information, student contact information, personal data, reports, student examination results etc

GDPR - General Data Protection Regulation
This policy document does not replace the Trust's or the School's GDPR Policy which must be read in conjunction with this policy.

RLT Staff IT Acceptable Use Policy

Staff User Agreement
(to be signed by the member of staff and returned for retention on their staff file)

As a school user of the network resources

I agree to;

- to follow the school rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult the IT Department or Line Management
- report any misuse of the network to the IT Department or Line Management.
- to report any websites that are available on the school Internet that contain inappropriate material to the IT Department or Line Management.

I will ensure that

- portable equipment such as cameras or laptops will be kept secured when not in use and to report any lapses in physical security to the IT Department or Line Management.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with IT Support and/or my line management.

I have read and understood

- the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
- the Trust's and the School's GDPR Policy
- The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.
- If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action.

Staff Name: _____

Staff Signature: _____

Date: _ _ /_ _ /_ _ _