Mission Statement
"A Caring Christian Family Where We Grow Together"

IT ACCEPTABLE USE PROCEDURE

Effective Date: 01/09/2017 **Review Date: March 2025 annual**

Review Date	Signed Executive Headteacher	Signed Director RCSAT
16/03/2020		
04/03/2021		
08/02/2022		
01/03/2023		
19/01/2024		

Persons Responsible for Policy:	Executive Headteacher RCSAT
Approval Date	16/03/2020
Signed:	Director RCSAT
Signed:	Executive Headteacher RCSAT

Information Technology (IT) resources, such as PCs, laptops, tablet devices and smart phones offer new and exciting ways of learning and working. We must also be aware that improper use can put our systems and information at risk.

This IT Acceptable Use Procedure aims to protect all users and minimise such risks by providing clarity on how to use IT Resources appropriately both in and out of the school environment.

The procedure will ensure:

- All users stay safe while using the internet and other IT Resources for educational use.
- That school IT resources and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That users are protected from potential risk in their use of IT in their everyday work.
- Users are aware of their responsibilities in the use of personal computer equipment (Laptops, phones, PCs, tablets etc.) for conducting school business.

'IT Resources' include all school equipment and information (all information systems, hardware, software and channels of communication, including mobile phones, social media, video, email, internet) and personal equipment such as mobile phones.

This procedure applies to all school employees, supply agency workers, governors, volunteers, educational consultants, and visitors with access to schools information and information systems.
They will be referred to as 'Users' in the purpose of this document.

The school will ensure that staff, governors and volunteers will have good access to IT to enhance their work, to enhance learning opportunities for our young people and will, in return, expect staff to agree to be responsible users.

All users of Rural Church Schools Academy Trust IT Resources are required to indicate that they understand and accept the terms of this agreement.

All users of Rural Church Schools Academy Trust IT Resources are aware of the following responsibilities:

- understand that IT includes hardware, software, the internet, email, social media and includes mobile phones, digital cameras, laptops and tablets.

- understand that it is a disciplinary offence to use the school IT equipment for any purpose not permitted by its owner.

- Will not disclose any passwords provided to them by the school.

- understand that they are responsible for all activity carried out under their username.

- will not install any hardware or software on any school owned device without the Principal permission.

- understand that their use of the internet may be monitored and if anything untoward is uncovered, could be logged and used in line with any disciplinary procedures. This includes all school owned devices. If an E-safety incident should occur, staff will report it to the Principal as soon as possible.

- will only use the school's email / internet and any related technologies for uses permitted by the Principal. If anyone is unsure about an intended use, they should speak to the Principal beforehand.

- will ensure that data is kept secure and is used appropriately as authorised by the Principal or Governing Body. No passwords should be divulged and laptops/memory sticks will be encrypted.

- When using school equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- will only use the approved email system for school business.

- Images will only be taken, stored and used for purposes within school unless there is parental permission for alternative use. At the start of each year, our parents are asked to sign if they agree to their children's images being used in our brochure or in the local press. If a parent does not agree to this, we ensure that their child's photograph is not used. Filming and photography by parents and the wider community at school events, such as sports days and school productions are the responsibility of parents and not the school. School is not responsible for images that may appear on social media which have been posted by parents or carers. When possible, a professional photographer will come to school to take photographs of children, for example in their play costumes. These will then be made available to parents.

- will report any incidents of concern regarding staff use of technology and/or children's safety to the Principal or Pastoral Manager with our school's Safeguarding Policy.

Specific Do's and Don'ts for IT Use are detailed here:

DO get the permission of your manager to take any confidential information home.
DO transport information from school on secure computing devices (i.e. encrypted laptops and encrypted memory sticks). Wherever possible avoid taking paper documents out of the office.
DO use secure portable computing devices i.e encrypted laptops or encrypted USB's when working remotely or from home.
DO use Onedrive on Office 365 to store documents securely, you can access these from any location on any device with a secure internet connection, save the changes in onedrive and not on your device.

DO use Security Pin Numbers on all staff ipads and personal mobile devices that are used for work emails, eg mobile phone
DO Log out or lock your PC or laptop when you leave your desk;
DO only use your allocated work email address as it is secure;
DO Use encrypted email for emailing personal data about a child;
DO use pseudonyms and anonymise personal data where possible.
DO ensure that access to SIMS, Teachers2parents (and all equivalent programs) are restricted to appropriate staff only and that leavers are removed in a timely manner.
DO ensure that all paper based information that is taken of premises is kept confidential and secure, ideally in a sealed envelope which indicates a return address if misplaced.
DO ensure that paper based information and laptops are kept safe and close to hand when taken out off premises. Never leave them unattended. Particular care should be taken in public places (e.g. reading of documentation on public transport).
DO ensure that when transporting paper documentation in your car that it is placed in the boot (locked) during transit.
DO return the paper based information to the School as soon as possible and file or dispose of it securely.
DO report any loss of paper based information or portable computer devices to your line manager immediately.
DO ensure that all postal and e-mail addresses are double checked to ensure safe dispatch of information. When sending personal information by post the envelope should clearly state 'Private – Contents for Addressee only'.
DO ensure that when posting/emailing information that only the specific content required by the recipient is sent.
DO Clear documents away at the end of the day or when leaving your desk. This stops people who are walking past your desk from reading things they shouldn't.
DO If you are regularly sending personal information to organisations outside of the school, ensure that you verify who you are contacting and password protect the document if necessary.
DO Take care when working from home. Your family members don't have a right to see the information you use for work

DO NOT put a forward on your work email to your personal email;
DO NOT open any attachments on suspicious emails or where you do not know who the sender is, delete from your system and report to the Data Protection Officer;
DO NOT use any pictures of children where they have their faces blurred out;
DO NOT unnecessarily copy other parties into e-mail correspondence.
DO NOT e-mail documents to your own personal computer.
DO NOT store work related documents on your home computer.
DO NOT leave personal information unclaimed on any printer or copier.
DO NOT leave personal information on your desk overnight, or if you are away from your desk in meetings.
DO NOT leave documentation or laptops in vehicles overnight.
DO NOT discuss case level issues at social events or in public places.
DO NOT put confidential documents in non-confidential recycling bins.
DO NOT print off reports with personal data (e.g. pupil data) unless absolutely necessary.
DO NOT use unencrypted memory sticks or unencrypted laptops

DO NOT Just because you have access to a system, this does not mean you have the right to access all of the information on it. Access is on a "need to know" basis.
DO NOT "Curiosity" checks are not permitted. You must have a genuine, legitimate work purpose to access information

- I understand that I am responsible for my actions in and out of school:

- I understand that this IT Acceptable Use Policy applies not only to my work and use of school IT equipment in school, but also applies to my use of school IT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment/role with the school.

- I understand that once I cease employment with the school/no longer act as Governor, I will ensure that any data I may hold that relates to my work within the school will be deleted or returned to the school and I will not retain any such information after this point.

- I understand that if I fail to comply with this IT Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police

I have read and understand the above and agree to use the school IT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Full Name _____

Signature _____

Date _____