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

SCHOOL HOMEWORKING PROCEDURE

Effective Date: 16/03/2020 **Review Date: Oct 2024 annual**

Review Date	Signed Executive Headteacher	Signed Director RCSAT
16/03/2020		
13/10/2021		
30/09/2022		
30/09/2023		

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

1. Introduction

Rural Church Schools Academy Trust is legally required, under the Data Protection Act 2018, to ensure the security and confidentiality of data we process on behalf of the public and our employees. This legal requirement also includes any data processed on the School's behalf by another organisation - a partner, contractor or supplier – regardless of where the information is processed, this includes when staff work from home or other remote locations.

Staff must also be aware that, even when working away from the office, everything they do remains subject to the Data Protection Act 2018 and the Freedom of Information Act 2002 in relation to all paper and electronic information that they create and receive as part of their employment with the School, regardless of where they work or store that information.

2. Purpose

This document gives general advice on the issues to consider to ensure that any School information you work on at home is protected from loss or unauthorised access and exploitation, while at the same time ensuring that it is accessible to anyone that needs to use it for their own work. Wherever possible, paper documents containing personal or sensitive information should not be transported out of the School environment and only electronic versions should be used.

This policy is a sub-policy of the Data Protection Policy.

3. Key Messages

This guidance is intended for all employees that work at home, either on an occasional or a regular basis, as well as Governors who may have cause to have access to documents of a sensitive or personal nature.

4. Scope

This guidance applies to all information in all formats, including paper files, electronic data, word processed documents and emails.

5. Definitions

Personal Information – Personal information is information that could adversely affect an individuals' privacy or which could harm an individual in some way, were it to be disclosed to unauthorised third parties either deliberately or accidentally.

Sensitive Information – Sensitive information is any other information that is of a confidential nature, which could cause harm to the School or any other third party (including other organisations or public bodies) if disclosed to an unauthorised third party either deliberately or accidentally.

6. **Key principles**

The following key principles underpin the School's policy on the storage, transmission and use of personal data and sensitive information outside the School's network environment. All staff must comply with these principles when using mobile devices and portable storage media or otherwise removing information outside the School's computing network environment.

- Avoid using personal data wherever possible
- If the use of personal data is unavoidable, consider partially or fully anonymising the information to obscure the identity of the individuals concerned.
- Use secure shared drives i.e. Office 365 to store and access personal data and sensitive information, ensuring that only those who need to use this information have access to it.
- Use secure shared drives i.e. Office 365 to access personal data and sensitive information instead of transporting it on mobile devices and portable media or using third party hosting services.
- If there is no option but to use mobile devices, portable media or email for high and medium risk personal data or information, only use encrypted laptops or memory sticks.
- Do not use personal equipment (such as home PCs or personal USB sticks) or third party hosting services (such as Google Mail) for personal data or information.
- Avoid sending high or medium risk personal data or information by email. If you must use email to send this sort of data, encrypt it. If you are sending unencrypted high or medium risk personal data or information to another RCSAT email account, indicate in the email title that the email contains sensitive information so that the recipient can exercise caution about where they open it.
- Do not use high or medium risk personal data or information in public places. When accessing your email remotely, exercise caution to ensure that you do not download unencrypted high or medium risk personal data or business information to an insecure device.
- Consider the physical security of high or medium risk personal data or information, for example use locked filing cabinets/cupboards for storage.
- Implement the School's retention and disposal policies so that you do not keep personal data and information that you do not need.

7. **Home and Mobile Working**

Taking School information home will always involve an element of risk so you should think carefully about whether you need to do so.

The measures you take when working at home will depend on the nature and sensitivity of the information involved, and should take into account the cost of implementing precautions and the likelihood and consequences of someone gaining access to the information.

This guidance document applies specifically to work that you do at home. You can limit the need to take information home by using the secure shared drives i.e. Office 365.

7.1. Using Your Laptop

- Only use School encrypted laptops or encrypted USB's when working remotely or from home.
- Work directly via the secure shared drives i.e. Office 365. This reduces the need to take home electronic information or to store it there, addresses business continuity concerns and limits the security measures you will need to take with regard to electronic information.
- If you work on a laptop, do not use it to store the only copy of information as it is more vulnerable to loss or theft. Files should be kept on the School servers and not saved to your laptop hard drive. If you must take a file home ensure you back it up to the server as soon as you return to the office.
- Do not use a personal email account for school business - do not email documents or files to your personal email account or from your personal email account to your work account.
- Do not allow anybody else - friends, family, children etc – to access or use school equipment such as your phone, laptop or tablet.

7.2. Physical security

- Wherever possible avoid taking paper documents out of school.
- Records should be updated as soon as possible with any work that you do at home.
- When you work at home, security should be of the same standard as that which is provided in the School.
- Take care when transporting information to or from your home.
- If you travel by public transport, keep all School information to hand. Hold onto bags or laptops rather than placing them on luggage racks. Keep smaller storage media, such as portable drives, in secure compartments of bags, rather than in a jacket pocket.
- If you travel by car, lock School information in the boot. Do not leave it in plain sight.
- Dispose of School information securely and appropriately. For example, do not dispose of documents you no longer need in general waste or recycling bins; use a shredder if you have one at home.

8. High and medium risk information

- High risk information should never leave the office in physical format. The only exceptions to this are members of staff who need to take high risk information away from Council premises as a necessary part of their job, such as social workers and solicitors, where electronic versions are not possible/available. If using high risk information away from the Council is an essential part of your job, ensure that you adhere to all sections of this guidance document. If you need to carry information with you, consider return it to the office at the end of your working day to store it securely, rather than taking it home.
- Do not use your own, non-School, desktop or laptop computer to store sensitive School information - you can avoid this by using remote secure access facilities.

- Your work area should be in a separate location to general 'living' areas. This location should not be able to be easily seen or accessed by people outside the home. For example, do not situate your work area or computer station next to a ground floor window.
- Make sure that information is not left where other occupants of your home can see it.
- Keep paper documents, files and portable media devices in a lockable cabinet and make sure that this is locked when not in use.
- Physically protect laptops. You can do this simply by placing it in a locked cupboard or drawer when not in use.
- If you are taking sensitive information home, in any format, go there directly. This reduces the chances of losing the information on the way.
- Use an appropriate carrier. Documents or other portable media should be transported in a secure, lockable briefcase or bag. Laptops must be carried in a laptop bag or rucksack.
- Exercise discretion. Do not read sensitive documents on a bus, for example, or work on personal data on a train. Do not draw attention to the fact that you are carrying School information.
- Access to secure storage facilities are provided to staff in all schools – tamba units, pedestal drawers etc.

9. Data Protection and Freedom of Information

The Data Protection Act 2018 and the Freedom of Information Act 2002 apply to all paper and electronic information that you create and receive as part of your employment, regardless of where you work or store that information.

The Data Protection Act sets out how organisations can handle personal data and gives an individual the right to access personal information held about themselves. The Freedom of Information Act entitles anyone from anywhere in the world to request access to any information held by the School. It also includes a statutory code of practice on records management which describes the systems we should have in place for managing our information. These pieces of legislation are as applicable to the work you do at home as the work you do on School premises, so you must therefore take this guidance into account when working at home

A failure to safeguard personal data at home could breach the Data Protection Act. In addition to financial penalties, a data protection breach could cause serious harm to the School's reputation and damage its relationship with a range of stakeholders. Following this policy enables you to access confidently the information you need to do your job and safeguards your information against loss, theft and corruption.

10. Failure to Comply

If you fail to follow the standards of conduct set out in this policy, or the IT Acceptable Use Policy, use of ICT systems may be withdrawn from you and/or disciplinary action taken against you, up to and including dismissal.

Failure to take adequate steps to protect and/or secure School ICT property, including but not limited to mobiles, laptops, tablets etc, may result in the individual being asked to reimburse the School for the loss if it is determined appropriate steps had not be taken.