ST TERESA of CALCUTTA
Catholic Academy Trust

Remote Support Policy

Policy Level	Trust/Statutory	**Ref No**	IT10
Approved by	RAR	**Approved date**	02.07.24
Responsibility	Head of I.T	**Next review date**	01.07.25
Published location	Shared Policy Folder		
Version number	**Date Issued**	**Author**	**Update Information**
1.1	08.11.24	Murray Leach	

Our Mission and Values

Our Mission

Our Trust Mission is simple, it is to make Christ known, making lives better for our communities, our children, and our young people.

Commitment to Equality

We are committed to providing a positive working environment which is free from prejudice and unlawful discrimination and any form of harassment, bullying or victimisation.

We have developed a number of key policies to ensure that the principles of Catholic Social Teaching in relation to human dignity and dignity in work become embedded into every aspect of school life and these policies are reviewed regularly in this regard.

Our Values

Hope

Inspired by St Teresa of Calcutta, we are people of hope. We have a complete belief in the future we will build together. By offering our children, staff and schools' opportunities to grow and flourish, we make aspiration and ambition a reality. Our people, just like St Teresa are relentless and fiercely ambitious. We will always reach for that which seems to be just out of our grasp.

Courage

As modelled for us by St Teresa of Calcutta, we will have the courage to do what is right. As a community, we will not shy away from making decisions that ensure our communities thrive. We will be brave in our actions. As a truly Catholic organisation this courage will be most apparent in how we collectively support the most vulnerable.

Innovation

St Teresa of Calcutta changed the world. Together, we will always be pursuing new ideas and best practice in all areas of our work. We will prepare our children and young people for the world that awaits them. A world which they will shape and change.

Contents Page

1.0 Policy Statement

St Teresa of Calcutta Catholic Academy Trust (STOCCAT) is committed to providing secure and reliable remote support for its staff. This remote support policy outlines the standards and procedures for remote support to ensure the security of private/sensitive information being processed by STOCCAT staff. All employees, contractors, and partners providing/receiving remote support must adhere to this policy to protect the data and resources of STOCCAT.

2.0 Purpose

This policy applies to all STOCCAT employees, contractors and partners who provide/receive remote support for computing equipment. Remote support is provided primarily by the IT department as a method of resolving/investigating IT issues/requests as an alternative to an onsite visit.

3.0 Scope

This policy applies to remote support procedures provided by STOCCAT and its employees, contractors, and partners. It covers all methods of remote support regardless of which support tools are used.

4.0 Definitions

- **Remote Support**: The ability to provide support services via network connectivity using remote support access software. Access can be via STOCCAT's internal network of via the internet.
- **Virtual Private Network (VPN)**: A secure network connection established over the internet that encrypts data between the user's device and the school's network.
- **Cloud-Based Services**: Online services provided through the internet, such as Microsoft 365, SharePoint, OneDrive, and other Office 365 applications.
- **Multi-Factor Authentication (MFA**): A security system that requires more than one method of authentication to verify the user's identity for a login or other transaction.
- **Encryption**: The process of converting information or data into a code to prevent unauthorized access.
- **Conditional Access Policies**: Policies set in Azure Active Directory that control access to cloud services based on conditions such as user location, device compliance, and MFA.
- **Remote Support Policies**: Policies set in the remote support software that determine whether a computer user is supported via Proctored or Open access.
- **Proctored Access**: A remote support access method that requires the user to acknowledge and allow connectivity to their computing device.
- **Open Access**: A remote support access method that does not require a user to allow access to their computing device.

- **Active Directory (AD) Security Groups**: Groups within Active Directory used to manage and control user access to resources and services.

5.0 Remote Support Methods

5.1 Cloud-Based IT management application: Remote support via cloud-based applications. Client devices need to be added / registered before connectivity can be established. The STOCCAT standard application is Senso, however other applications can be utilized where Senso is not available.

5.2 Microsoft Teams: Screen share / control facility from within Microsoft Teams application.

5.3 PC to PC RDP connection: Remote support via built-in windows connectivity tool.

6.0 Security Measures

6.1 Proctored access: Security policies are in place within Senso to force proctored access for defined devices. Remote support requests will be made to the end user via a pop-up message that that an IT engineer requires access to take control of their computing device. The end user must acknowledge and allow the connection. Prior communication should be made between the IT engineer and end user to confirm that a remote support session needs to be used. If the connection is rejected the connection will not be established. The IT end user may end the session at any time.

6.2 Defined devices can be added / removed from security group as required. A list of defined devices should be provided by the school SLG and reviewed at regular intervals to ensure it is current.

6.3 Encryption: While no specific encryption protocols are mandated, it is recommended that remote connections use encrypted channels where feasible.

7.0 Access Control

7.1 Cloud-Based IT management application Access: Access to this application is restricted to the IT department. Remote support access is granted to all IT Support engineers. Access is managed through the application management portal.

7.2 User Access: Remote support is available only to STOCCAT provided devices.

7.3 Authorization: Access must be authorized by the IT department and is subject to regular reviews.

8.0 Monitoring and Compliance

8.1 Application Logs: Application activity logs are used to monitor remote access to cloud services.

8.2 Compliance Checks: Regular audits are conducted to ensure compliance with this policy.

9.0 Incident Response

9.1 Incident Response Procedures: In the event a user suspects an incident of unauthorized access, the IT department should be made aware, and a security incident will be raised. The procedures outlined in the Incident Response Policy must be followed.

10.0 User Training

10.1 Training Requirements: Although no formal training is currently in place, users are encouraged to follow best practices for secure remote support. The IT department will provide guidelines and resources to support this.

11.0 Device Management

11.1 Device Requirements: Only STOCCAT provided devices will be used in remote support sessions. User devices require a software client and license to be allocated to it. Personal devices will not be supported via remote support functions.

12.0 Review and Updates

12.1 This policy must be reviewed annually and updated as necessary to reflect changes in legal requirements and best practices.

12.2 Changes to this policy must be communicated to all employees, contractors, and partners.

13.0 Policy Compliance

13.1 Compliance Measurement

The STOCCAT IT Dept will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner

13.2 Exceptions

Any exception to the policy must be approved by the IT Dept in advance.

13.3 None-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment

14.0 Related Standards, Policies and Processes

- Acceptable Use Policy
- Device Management Policy
- Access Control Policy
- Incident Response Policy