The Park Federation

The Park Federation Academy Trust

Remote Access Policy 2023

Version History

Version	Date	Status and Purpose	Changes overview
1	September 2019	Review	
2	July 2020	Periodic review	KCSIE 2019
3	July 2021	Periodic review	KCSIE 2020
4	September 2022		
5	September 2023	Periodic review	

Approval History

Signed by the CEO and Federation Principal on behalf of the Board of Directors

Dr. Martin Young

Date of approval September 2023

Date of review September 2024

Notes on Document Control

This document is the property of The Park Federation Academy Trust and its contents are confidential. It must not be reproduced, loaned or passed to a 3rd party without the permission of the authoriser.

It is controlled within the Park Federation Academy Trust Admin Server where the electronic master is held and can be accessed on a read only basis, subject to security permissions.

Users of the document are responsible for ensuring that they are working with the current version.

Paper or electronic copies may be taken for remote working etc. However, all paper copies or electronic copies not held within the Admin Server are uncontrolled. Hence the footer ‘DOCUMENT UNCONTROLLED WHEN PRINTED’ which must not be changed.

Once issued, as a minimum this document shall be reviewed on an annual basis by the originating team/function. Any amendments shall be identified by a vertical line adjacent to the right hand margin.

To enable continuous improvement, all readers encouraged to notify the author of errors, omissions and any other form of feedback.

Contents

Legal Framework:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools

Associated Documentation and Policies: The Park Federation Academy Trust (TPFAT) Policies. Disciplinary Policy, Data Protection Policy, On line Safety Policy, Remote Access Policy, Staff Code of Conduct, Social Media Policy. Information shared is subject to copyright, data protection, freedom of information, equality, safeguarding and other legislation.

What is Remote Access?
Remote Access refers to any technology that enables you to connect users in geographically dispersed locations. This access is typically over some kind of dial-up connection, although it can include Wide Area Network (WAN) connections.

1. Purpose of Policy

Remote access by staff is a method of accessing files and systems that is becoming more common in education. In The Park Federation Academy Trust, the benefits of securing remote access are considerable – business can be conducted remotely with confidence and sensitive corporate information remains confidential. This document sets out the policy for remote access and includes a set of common controls, which can be applied to reduce the risks associated with a remote access service.

Willful or negligent disregard of this policy will be investigated and may be treated as a disciplinary offence.

2. Scope

This policy covers all types of remote access, whether fixed or 'roving' including:

2.1. Travelling users (e.g. Staff working across sites or are temporarily based at other locations)

2.2. Home workers (e.g. Teachers or Admin staff)

2.3. Non The Park Federation Academy Trust staff (e.g. Contractors and other 3rd party organisations)

3. Objectives

The objectives of The Park Federation Academy Trust's policy on remote access by staff are:

3.1. To provide secure and resilient remote access to information systems.

3.2. To preserve the integrity, availability and confidentiality of information and information systems.

3.3. To manage the risk of serious financial loss, loss of client confidence or other serious business impact which may result from a failure in security.

3.4. To comply with all relevant regulatory and legislative requirements (including data protection laws, safeguarding) and to ensure that the trust is adequately protected under computer misuse legislation.

4. Principles

In providing remote access to staff, the following high-level principles will be applied:

4.1. A senior member of the trust will be appointed to have overall responsibility for each remote access connection to ensure that the trusts policy and standards are applied.

4.2. A formal risk analysis process will be conducted for each application to which remote access is granted to assess risks and identify controls needed to reduce risks to an acceptable level.

4.3. Remote users will be restricted to the minimum services and functions necessary to carry out their role.

5. Responsibilities

5.1. The Park Federation Academy Trust Finance and Operations Committee is ultimately responsible for ensuring that remote access by staff is managed securely.

5.2. The Park Federation Academy Trust Finance and Operations Committee will maintain this policy, standards and procedures for remote access to ensure that risks are identified and appropriate controls implemented to reduce those risks.

5.3. The Park Federation Academy Trust Finance and Operations Committee is responsible for confirming whether remote access to business applications and systems is permitted.

5.4. The IT Network Manager is responsible for providing authorisation for all remote access users and the level of access provided.

5.5. The IT Network Manager will ensure that user profiles and logical access controls are implemented in accordance with agreed access levels.

5.6. The IT Network Manager will provide assistance on implementing controls.

5.7. The IT Network Manager is responsible for assessing risks and ensuring that controls are being applied effectively.

5.8. All **remote access users** are responsible for complying with this policy and associated standards. They must safeguard corporate equipment and information resources and notify The Park Federation Academy Trust immediately of any security incidents and breaches.

5.9. Users must return all relevant equipment on termination of the need to use remote access.

6. Risks

The Park Federation Academy Trust recognises that by providing staff with remote access to information systems, risks are introduced that may result in serious business impact, for example:

6.1. unavailability of network, systems or target information

6.2. degraded performance of remote connections

6.3. loss or corruption of sensitive data

6.4. breach of confidentiality

6.5. loss of or damage to equipment

6.6. breach of legislation or non-compliance with regulatory or ethical standards.

7. Security Architecture

The security architecture is typically integrated into the existing The Park Federation Academy Trust network and is dependent on the IT services that are offered through the network infrastructure. Typical services include:

7.1. Password authentication, authorisation, and accounting

7.2. Strong authentication

7.3. Security monitoring by intrusion detection systems
7.4. Multi Factor Authentication

8. Security Technologies

To ensure the most comprehensive level of protection possible, every network should include security components that address the following five aspects of network security.

8.1. User Identity

All remote users must be registered and authorised by the IT Network Manager. User identity will be confirmed by strong authentication and User ID and password authentication. The IT Network Manager is responsible for ensuring a log is kept of all user remote access.

8.2. Perimeter Security

The IT Network Manager will be responsible for ensuring perimeter security devices are in place and operating properly. Perimeter security solutions control access to critical network applications, data, and services so that only legitimate users and information can pass through the network. Routers and switches handle this access control with access control lists and by dedicated firewall appliances. Remote Access Systems with strong authentication software control remote dial in users to the network. A firewall provides a barrier to traffic crossing a network's "perimeter" and permits only authorised traffic to pass, according to a predefined security policy. Complementary tools, including virus scanners and content filters, also help control network perimeters. Firewalls are generally the first security products that organisations deploy to improve their security postures.

8.3. Secure Connectivity

The Park Federation Academy Trust will protect confidential information from eavesdropping or tampering during transmission.

8.4. Security Monitoring

Network vulnerability scanners will be used to identify areas of weakness, and intrusion detection systems to monitor and reactively respond to security events as they occur.

8.5. Remote diagnostic services and 3rd parties

8.5.1. Suppliers of central systems/software expect to have dial up access to such systems on request to investigate/fix faults. The Park Federation Academy Trust will permit such access subject to it being initiated by the computer system and all activity monitored.

8.5.2. Each supplier or The Park Federation Academy Trust user requiring remote access will be required to commit to maintaining confidentiality of data and information and complying with safeguarding. Ensuring no one else is able to view the data.

8.6. User Responsibilities, Awareness & Training

The Park Federation Academy Trust will ensure that all users of information systems, applications and the networks are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities. Irresponsible or improper actions may result in disciplinary action(s). Staff must ensure that the latest antivirus software and firewalls are in place when working from home on personal devices.

9. System Change Control

All changes to systems must be recorded on a System Change Control form and authorised by the The Park Federation Academy Trust, Finance and Operations Committee.

10. Reporting Security Incidents & Weaknesses

All security weaknesses and incidents must be reported to the IT Network Manager.

11. Guidelines, training and compliance

The IT Network Manager will produce written guidance and training materials for all remote access users. Staff are to access the system as though they were at work and ensure that data is not visible to others.

12. Validity of this Policy

This policy should be reviewed annually under the authority of the Chief Executive Officer. Associated information security standards should be subject to an on-going development and review programme.