INVICTUS
Education Trust

GDPR ACCESS CONTROLS & PASSWORD POLICY

Approved by Board of Trustees
25 May 2021

To be reviewed by Board of Trustees
April 2023

Document Provenance

GDPR Access Control & Password Policy	
Committee Approval Level	Board of Trustees
Policy Author/Responsibility	Chief Operating Officer – Julie Duern
Policy First Implemented	July 2018
Frequency of Review	Every 2 Years
Next Review Date	April 2021
Policy Approved by Committee	25 May 2021
Next Review Date	April 2023

Content **Page**

1. Policy Statement 3
2. Purpose 3
3. Scope 3
4. Objectives 3
5. Procedures, Controls and Measures 4
    5.1 Logical Access Control 4
    5.2 Passwords 5
    5.3 User IDs & Badges 7
    5.4 Privileged Accounts 7
    5.5 Authorised Access 7
    5.6 Physical Access Controls 8

6. Responsibilities 9

1. POLICY STATEMENT

It is the Trust's policy to protect and secure the information and systems within our remit and we take this function very seriously. We have developed and implemented several physical, logical and procedural measures and controls to enforce our approach. We understand that it is vital to protect the systems and information held and used by us from unauthorised use or access and are fully aware of how such access can affect security, personal information and individuals. The types of measures and controls used by the Trust are:

- **Physical Access Controls** ensuring the availability of systems and information is restricted to authorised persons only, thus preventing locations and information from being accessible to non-authorised individuals. Premises security measures include gates, alarms, CCTV, key-card access, buzzer systems, deadbolts, locks on doors/windows etc.
- **Logical Access Controls** utilise tools and protocols for identification, authentication and authorisation of our computer information systems (*including remote access, laptops and phone systems*). The Trust's logical access controls enforce access measures to our systems, programs, processes, and information and include password protocols, user authentication methods, data and authentication credentials encryption and network, system and user-level firewalls.
- **Procedural Access Measures** include our defined policies and procedures that are followed by all staff and third parties and provide the steps for areas such as access control, information security, password protocols and clear desk measures.

2. PURPOSE

The purpose of this policy is to ensure that system based and physical access to any information, location and/or system is controlled and where applicable restricted using controls and procedures that protect the associated information systems and data. The Trust is committed to the security of the information and assets within our remit and enforce and stress test all access measures to ensure their functionality, effectiveness and purpose.

This Access Control & Password Policy aims to restrict access to controlled information and/or systems to only those staff or third parties who are authorised or have written permission from the Trust. Where temporary and/or partial access to information or systems is required, we follow strict protocols, to only enable, access to the information, or for the duration required, by the activity.

3. SCOPE

This policy applies to all staff within the Trust (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Trust in the UK), and pertains to the processing of personal information. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

4. OBJECTIVES

The Trust is committed to ensuring compliance with the rules, standards and regulations as laid out by its regulating and governing bodies and confirms that it has developed and implemented the appropriate procedures, systems, controls and measures to manage and mitigate against risk.

For systems containing restricted and personal information and data, an access control matrix must be developed to record role based authorised access recorded on an individual basis. Authorisation procedures must be in place for managers to authorise all access (*including short term and temporary*

access) recorded on the matrix. The access matrix must be continually updated and maintained to reflect accurate records of access.

The Trust has a full understanding of the compliance standards that we are obligated to meet and confirm that we have in place effective and efficient tools and controls for meeting these obligations under the current regulatory system.

The Trust's objectives regarding compliance are to:

- Allow staff to gain access to specific systems and information, which is determined by the IT Network Managers and the Senior Management Team
- Generic logons are not permitted across the Trust systems, however, use of generic accounts under 'controlled' circumstances can be permitted at the discretion of the IT Network Managers
- To ensure relevant education/company, contractual, regulatory and legislative security standards are met and adhered to, employee screening checks, including DBS, and referencing are undertaken if required.
- The appropriate level of access to systems and information will be determined based on the employee's user-level, role-based requirements and ad-hoc job functions and roles.
- If authorisation to use systems and information is granted, unique logon credentials and password will be provided to the employee, utilising the strong password controls detailed in this policy.
- Access for remote users shall be subject to authorisation by the IT Network Managers.

5. Procedures, Controls and Measures

It is pivotal to educating children and operating the business of the Trust that the Trust uses computers, telephone systems, software, hardware devices and data storage systems. Such systems are used to store information and assets that are of a personal and confidential nature. It is therefore essential that we protect and secure such information and therefore access to the systems using a variety of access controls and measures.

We take a multi-tiered approach when securing systems and restricting access and detailed in this policy are the procedures and methods used throughout the Trust. This information is disseminated to all employees and forms part of our information security program.

5.1 Logical Access Control

Access to systems within the Trust are governed by our tiered logical access control measures. Access to any system is classified as one of the below access levels and restrictions are implemented at the user level. Levels can be changed at the discretion of the IT Network Managers. Considerations for granting access is assessed based on:

- An employee or user's need of access to complete their job and/or task
- Duration of access
- Level of access
- Information types located on the system in questions
- Security measures in place if access is granted
- Ability to remove access at a predetermined time

- Access is decided and allocated on a case-by-case basis and can only be assigned by the IT Network Managers.

5.1.1 ROLE-BASED ACCESS

Users are identified as being part of a school group/employee group and their level of access to Trust/School systems is determined in relation to their role and responsibilities within the Trust. Such group access is considered necessary for each employee to enable them to carry out their job and includes access to areas such as internet, intranet, email, printers, phone systems, security systems etc.

5.1.2 MANAGER ACCESS

System access is granted at a higher level for Headteachers and Senior Managers who can access more system areas than generic employees can. Such access is deemed essential to their oversight role and enables managerial staff to carry out functions and processes that require access to personal information, secure systems or data.

5.1.3 INDIVIDUAL ACCESS

System access is granted at the required level based on an educational/ business and/or legal requirement and is only granted to the individual(s) who require access (*i.e. if an employee is granted extended access, this is not inherited by any other role-based group member*). Such access may include a role-based user needing access to sensitive information or restricted systems to perform a task or one-off project.

5.2 PASSWORDS

Passwords are a key part of the Trust's protection strategy and are used throughout the Trust to secure information and restrict access to systems. We use a multi-tiered approach, which includes passwords at user, management, device, system and network levels to ensure a thorough and encompassing approach.

Passwords afford a high level of protection to resources and data and are mandatory requirements for all employees.

5.2.1 PASSWORD CREATION & CHANGE

Only those authorised to access specific devices, information, systems are provided with the relevant passwords, and such provisions are reviewed regularly to ensure that access is still valid and required. Employees may never share their passwords with anyone else in the Trust, including co-workers, managers or IT staff and unique passwords are used for all employees and access to systems and devices.

Employees are made aware that strong passwords are required for all systems and user-access and that a strict non-disclosure protocol applies to passwords. Where applicable to the system or device being used, the Trust utilises software to enforce the use of strong passwords. Employees are not allowed to share or disclose any password.

Strong passwords are enforced on systems and by users and must be:

- More than 8 characters
- Include letters, numbers and at least 1 special characters
- Not be easily recognisable *(i.e. no names, dates of birth, places etc*)

- Must include upper and lowercase letters

All passwords are changed termly, and users are not permitted to reuse the same password within a 1-year period. This is forced using software on all systems and a password change is automatically promoted at the start of each term. This change is enforced within 5 days of the change reminder being shown.

If a password is forgotten, only the IT Network Managers can reset the passwords. Passwords that have been forgotten are changed by default and cannot be reset to use the same password. A force change of password is also affected if the user suspects that the password has been compromised.

Where a password is reset, the individuals identify is first verified. This is essential where remote access passwords are changed or reset, and the IT Network Managers is not able to physically verify the identity of the user. A two-step identification process is used in such instances with user-known variables being asked and answers verified prior to passwords being reset and disclosed.

5.2.2 DEFAULT PASSWORDS

It is occasionally necessary to set up default password at the IT Manager level. This is usually only when a new system or user are being set up and a password change will be promoted from the first user use. Default passwords are change as soon as is possible and where applicable, access to information is restricted until a strong password has been created.

Where new systems, devices or software is purchased, default passwords are immediately changed and reset to use the strong variables indicated above.

5.2.3 PROTECTING PASSWORDS

The Trust is aware that viruses, software and phishing scams can attempt to obtain passwords at a user level. Whilst Firewalls are used to secure and protect systems and software, employees are provided with training and guidance on phishing and are instructed to neve disclose their passwords in a physical or online environment. This includes not disclosing passwords to third parties, clients or representatives who may have a legitimate need to access a system.

Password fields are always displayed in a star format (*****) so that clear text is not present when a password is typed. This helps to prevent unauthorised access or password disclosure by copy & paste or electronic printing methods.

Writing down or storing passwords in any written or digital format is forbidden and all employees are made aware of this. Disclosure or unintentional loss of a password that has been written down in any format will result in disciplinary action being taken.

If a user fails to use the correct username and/or password when logging in to a system or device, we utilise generic failure messages that do not disclose the exact nature of the login error. After three failed attempts, the system will advise that login has failed, however it will not disclose if this is due to the username, password or both being incorrect. This aids in preventing brute force attacks or a non-authorised user being aware of which field is incorrect, which then increases their login attempts.

Where login fails, we operate a three-strike approach and the system will become unavailable for 15 minutes before the login can be re-tried. This protects against external ‘bot’ attacks and brute force.

5.3 User ID's and Badges

The Trust has adopted ID badges for all employees, visitors and third parties who are in our school buildings. Such badges are specific to those they are assigned to and ID's or badges not in use are stored in a secure, locked area.

Employees must wear their ID badge at all times whilst in the school or whilst visiting third-party offices and are not allowed to share or copy their badge. All ID badges are assigned a unique verifying employee code, which is specific to the employee and is logged on an Access Control Register. If an employee loses their ID, their code is immediately deactivated, and a new code is assigned. Codes are never reused after deactivation.

Visitors to the Trust are issued with a Visitor ID Badge, which states their name, company, position and responsible person. Visitors are accompanied on school premises at all times and are required to log in and out of the building, sign confidentiality agreements and are assigned a Trust employee who is responsible for them during their visit.

5.4 Privileged Accounts

The Trust understands the extreme importance of securing and restricting access to privileged accounts. Such accounts enable direct access to our network, servers, firewalls, routers, database servers, systems and software and as such are treated with the utmost security and protection. Employees and third parties are never given access to privileged accounts, unless they have been assigned responsibility for a direct function. If this the case, access is only given to the exact system or infrastructure required to complete their task.

We audit access to privileged accounts on a weekly basis and review access monthly to ensure that it is still required or is of use. Logs of access to privileged accounts are reviewed for consistency with access records.

5.5 Authorised Access

The Trust keeps an Access Register and details which employees or third parties have access to which systems and information. The register also notes when the access was given, when it will be restricted (*if temporary access*), the type of data or system being accessed and the reason for access.

5.5.1 Login Controls

Systems can only be accessed by secure authentication of user validation, which consists of a username and password at the role-based user level. All computers have an active firewall and default to a lock screen with user authentication required after 10 minutes of inactivity. All staff are aware that if they leave their workstation, their monitor is to be turned off and their system locked. All computers are closed-down at the end of the day and are not allowed to be left running during 'out of business' hours.

5.5.2 Credentials & Roles

Access to any systems within the Trust (*including sending email*), utilises authentication based on the valid credentials being used. Each user is assigned unique credentials and are not allowed to share or disclose them to any other employee or third party. It is necessary for credentials to be stored so that when they are used to access a system, database or send an email, the authentication process works. All authentication credentials are encrypted when stored and transmitted and access is restricted to the IT Network Managers.

5.6 Physical Access Controls

Access to the Trust premises are protected by our building access controls. These increase building, information and employee security, safety and ensure that no unauthorised access is possible.

5.6.1 Door & Window Controls

The Trust has robust site security measures in place across its schools, which includes, intruder alarms, keypad access, CCTV etc.

All windows are kept locked when the building is vacated and intruder alarms set. Windows open during the day are secured with restricted access hinges to prevent access. Visitors are escorted at all times during a visit and are given an ID badge.

When the school has been vacated at the end of school day/working hours, the alarm system is activated and all windows and doors are locked. The building is 'locked down' and any alarm trigger will immediately notify the Security Services who have a contact for the relevant school and the relevant member of staff.

5.6.3 Direct Access

The use of keys to any buildings, rooms, secure cabinets, safes etc are always controlled and recorded and keys are only provided to employees who require them for educational/business and/or legal reasons. When not in use, keys are stored in a secure, locked cabinet and only the senior manager has access. Locations of keys are known at all times and if there is any suspicion that a key has been lost or compromised, lock and access points are changed immediately and monitored until the change is affected.

Visitors are not permitted to access server, network or confidential information areas without prior authorisation. Where authorisation has been given, visits are always escorted by a manager or the designated member of staff.

5.7 Leavers & End of Contract

We operate an immediate deactivation process of any credentials and access rights on termination of contract.

Leavers are required to turn in their ID badge before existing the school building. Hard copy ID's are destroyed and where applicable, any electronic ID's are deactivated with immediate effect. It is the line manager's responsibility to ensure that ID badges are returned.

Where a project or service contract ends, any access or credentials provided during the contract are deactivated and any ID badges or keys are returned and signed back into the logbook.

Where an employee is on annual leave, we can suspend their credentials and access rights and reactivate on their return. This reduces the risk of unmanned access points, but also prevents having to reset up new credentials and access levels.

6. Responsibilities

IT Network Managers are responsible for ensuring that all staff and managers are aware of security policies, including access control and secure passwords and the Trust operates a top-down approach. Managers need to be aware they have a responsibility to ensure staff have sufficient, relevant knowledge

concerning the security of information and systems, and new starters and existing staff training workshops are run on an annual basis covering the access control and password policies and objectives.