Welland Park Academy

I.T. KEY PROCESSES

Starters, Leavers & VPN Access

2024-25

Reference this policy is aligned to with LCC	**n/a**
Agreed with Support Staff Trade Unions	**n/a**
Adopted by the Governing Body	**Mar 21**
Next Review Due	**Sep 25**
Agreed with Teacher Trade Unions and Professional Associations	**n/a**

Initial summary

The Academy has a responsibility to protect its reputation as well as safeguarding individuals. We look to do this by giving the correct access to school systems through a detailed process of approved access.

This policy provides a clear process of allocation and then removing access where there is a required need. The option to request VPN access and how it is granted is also documented.

Scope

This policy applies equally to everyone who reads or processes Academy information, including:

- All staff, whether permanent, temporary or casual;
- All governors;
- All volunteers;
- LA staff working on site (e.g. LEAMIS technicians, Group Bursar Service, etc);
- Contractors and consultants; and
- Partners and suppliers

Throughout this document the words “employee”, “staff” and “user” are used to cover all of these groups of people.

Purpose

The purpose of this policy is to:

- Protect the Academy’s information and subsequently to protect the Academy’s reputation;
- Enable secure access sharing to deliver services;
- Protect the Academy from legal liability and inappropriate use;
- Encourage consistent and professional use of information and systems;
- Ensure everyone is clear about their roles in using and protecting individual access;
- Maintain awareness of information security;
- Protect the Academy’s employees
- NOT constrain reasonable use of information & access in support of normal business activities of the Academy.
- This policy shall be seen as additional to all other Academy policies relating to information disclosure and personal conduct.

This policy should be read in conjunction with:

- Acceptable use Policy
- CCTV Policy
- Whistleblowing Policy
- Information Security Policy

Roles and responsibilities

All Information Users

- Comply with this policy and related processes, procedures and guidelines.
- Comply with legal, statutory, regulatory and contractual obligations related to information.
- Be familiar with the operation and security requirements of the information and computer systems, to minimise the possibility of harm to confidentiality, integrity and availability.
- Observe the utmost care when dealing with personal and sensitive information to ensure that it is never disclosed to anyone inside or outside the Academy without proper authorisation.
- Report immediately to the Principal (or otherwise, in accordance with the Whistle Blowing Policy) all suspected violations of this and all other security policies; system intrusions; and any other security incident or weakness which might jeopardise the Academy's information, access or information systems.
- Read and act on any communications and training regarding information security, seeking clarification if these are not understood.
- Play an active role in protecting information & access in day-to-day work.

Governors and SLT

- Approve this policy.
- Implement and promote Information & Access Security to all staff within their service areas.
- Ensure that employees understand and abide by the Information Security Policy and its associated policies, processes, procedures, guidelines and understand its impact.
- Assign owners to all information & access in their area of responsibility.
- Provide effective means by which all staff can report security incidents and weaknesses, and act on all such reports according to agreed incident management policies and processes.
- Apply security controls relating to Human Resources and ensure that job descriptions address all relevant security responsibilities.
- Provide written authorisation for access to information & access.
- Ensure that communications regarding information security are cascaded effectively to all staff.
- Ensure that information security is an integral part of all departmental processes

IT Services

Be the custodian of electronic information & access in its care by implementing and administering technical security controls as appropriate.

- Assist Information Owners in identifying technical information security risks and appropriate technical security controls.
- Assist Welland Park Academy to ensure all software is licensed and remove unlicensed software.
- Provide contingency arrangements for information systems.
- Provide appropriate protection from malicious software.
- Monitor and report breaches of this policy including unauthorised attempts to access information or systems.
- Monitor and investigate technical security breaches.
- Provide technical support to enable compliance with this policy.

Processes and procedures

New Starter

Before a new member of staff can start their employment at Welland Park Academy, their details are entered onto the MIS system (SIMS) to generate a contract. Once approved by the DFO a creation request is generated and sent to a software package called Locker.

Locker generates an access account with a temporary password for which IT Services receive a notification. They will then activate the new user by viewing the roles and responsibilities and applying the relevant access.

A typical user would get access to Microsoft 365, SIMs (role dependent access) and EduLink One (role dependent access).

All roles currently have a selection of software that they will require for their role. Some of the key main ones are: *

- FMS
- SIMs
- CPOMs
- Every Education
- Active Learn
- Kerboodle
- ~~MathsWatch VLE~~
- EdulinkOne
- Microsoft 365
- Leicestershire Traded Services
- Provision Map (SEND)
- School Bus
- 4 Matrix

*this list is not exhaustive.

In most circumstances there would be a handover of key knowledge and resources from the current to the new postholder. Where this is not possible, it is the responsibility of the Line Manager to ensure all necessary access is given.

IT Services look to mirror the exiting member of staff's access or if it is a new role they seek approval from the HR Manager, Director of Finance & Operations or the Principal.

Leavers

When a member of staff ceases to be an employee of Welland Park Academy, all access arrangements for them need to be removed from all Academy systems as well as ensuring that all academy data is kept securely.

Leavers will be expected to share their password safety systems (vaults, potentially on personal devices) to demonstrate that all Welland Park Access has been deleted and removed.

Welland Park Academy reserves the right to enforce a factory reset of any member of staff's personal device if they do not comply with the exit process. This can be actioned via Microsoft Azure if the member of staff has used their work account on the device (This course of action will have been agreed when the account has been added onto the personal device).

Keeping Access & Systems Secure

Employees are expected to take appropriate measures to ensure the security of personal access at all times, including keeping passwords secure potentially using password vault software and Two-factor Authentication (2FA) were possible.

Computer screens should always be locked ("Windows" + "L") if being left switched on and unattended. Access will be afforded on a "need to do" basis, and access of leavers removed promptly.

Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons or members of the public.

Passwords

Passwords must not be shared with other members of staff under any circumstances.

Passwords should not be written down and/or left on display or be easily accessible.

Passwords must be "complex", as we have password policies in place to enforce this. Passwords must contain upper and lower case letters, as well as numbers and special characters. They must be at least 12 characters long, without containing basic information such as the user's name.

This policy applies to a user's school computer account, and in turn their Microsoft 365 (Teams, emails, etc,) and EduLink One. This policy does not apply to any other online learning platforms, as they will each have their own password policies in place.

~~Staff are also required to change their passwords every 90 days in accordance with this policy.~~

The "remember password" feature should never be used.

Staff are encouraged to password protect any personal files, in particular those that contain potentially embarrassing information about an individual or an organisation.

VPN Access

Not all roles and contractors are able to have VPN access.

Current roles & contractors that can request access are:

- Principal
- Vice Principal
- Assistant Principal
- Director of Finance & Operations
- School Business Manager
- Network Manager
- Assistant Network Manager
- Data Manager
- Exams Officer
- SENDCO
- Principals PA
- Rydal Communications (If their services need it, it is granted and monitored)
- Wavenet (If their services need it, it is granted and monitored)
- ~~Proband (If their services need it, it is granted and monitored)~~
- Leicestershire Cyber Crime Unit (If their services need it, it is granted and monitored)
- LEAMIS (If their services need it, it is granted and monitored)
- Edulink One (If their services need it, it is granted and monitored)

Business reasons and approvals for VPN access

ROLE	REASON FOR VPN ACCESS	APPROVED BY
Principal	Running the School, keeping on top of all issues and giving a better work life balance to enable them to work from home.	Chair of Governors
Vice Principal	Running the School, keeping on top of all issues and giving a better work life balance to enable them to work from home.	Principal
Assistant Principal	Running the School, keeping on top of all issues and giving a better work life balance to enable them to work from home.	Principal
Director of Finance & Operations	Running the School, keeping on top of all issues and giving a better work life balance to enable them to work from home.	Principal
School Business Manager	Running the School, keeping on top of all issues and giving a better work life balance to enable them to work from home.	Director of Finance & Operations

Network Manager	Running the School, keeping on top of all issues and giving a better work life balance to enable them to work from home.	Director of Finance & Operations
Assistant Network Manager	Running the School, keeping on top of all issues and giving a better work life balance to enable them to work from home.	Director of Finance & Operations
Data Manager	Granted at peak times due to workload around key returns. Access is removed when not required.	Vice Principal
Exams Officer	Granted at peak times due to workload around key returns. Access is removed when not required.	Vice Principal
SENDCO	Running the SEND department, keeping on top of all issues and giving a better work life balance to enable them to work from home.	Principal
Principals PA	Running the School, keeping on top of all issues and giving a better work life balance to enable them to work from home.	Principal
Rydal Communications	Granted to support the school with all WatchGuard firewall issues, when needed.	IT Services, Director of Finance & Operations.
Wavenet	Granted to support all server and Microsoft product issues. (Service contract)	IT Services, Director of Finance & Operations.
~~Proband~~	~~Granted to support all server issues (reserve service provider)~~	~~Network Manager, Director of Finance & Operations, IT Technicians.~~
Leicestershire Cyber Crime Unit	Granted to support the school with anything relating to a Cyber Attack.	IT Services, Director of Finance & Operations.
LEAMIS	Granted to support the school with key MIS system issues.	IT Services, Director of Finance & Operations.
EduLink One	Granted to support the school with the software that we communicate to parents and students with. It covers parents' evenings, notifications, homework & data management.	IT Services, Director of Finance & Operations.

Disposal of digital data and devices

All data, whether paper or electronic, must be disposed of properly and in accordance with the school's document retention and disposal schedule.

If a PC or laptop is to be given to another user, personal data should first be removed from it (e.g. student databases, free school meal information, etc)

PCs and laptops must be disposed of securely, through our current approved supplier list.

It is imperative that staff follow any guidelines issued when overwriting data. Sending information to a computer's recycle bin does not delete the data as such. It is therefore important to empty the recycle bin regularly.

Paper records containing personal data or confidential information must be shredded.

Monitoring

Use of access, electronic and non-electronic information and the use of information systems shall be monitored for the following reasons:

- To ensure adherence to this policy;
- To detect and investigate unauthorised use of information;
- To maintain the effectiveness, integrity and security of the computer network;
- To ensure that the law is not being contravened;
- To protect the services provided by the school to the public; and
- To protect the integrity and reputation of the school.

All monitoring shall be:

- Fair and proportionate to the risks of harm to the school's information and reputation;
- Undertaken so as to intrude on users' privacy only as much as is necessary;
- Carried out similarly regardless of whether the user is school-based or working remotely; and
- Carried out in accordance with legislative requirements.

Access to any records of usage will be stringently controlled.

Reporting security breaches

In the event of loss or theft of computer equipment the Principal must be informed at the earliest opportunity. Security issues should be raised with the Principal or Finance & Operations Director in the first instance. If this is not appropriate reference should be made to the whistleblowing policy.

Security incidents and weaknesses can be reported to the following:

- Principal
- Director of Finance & Operations
- LEAMIS helpdesk Telephone: 0116 231 1280 E-mail: helpdesk@leamis.org.uk
- The Information Security Consultant at County Hall on (0116) 305 7693
- Katie Robey, System Information Manager, Room G8, County Hall on (0116) 305 5783

Reports may be made by phone, face to face, or in writing.

Policy review

This policy shall be reviewed every two years.

This policy and its associated procedures and guidelines shall be updated according to:

- Internally generated changes (e.g. changes in organisation, technology, etc)
- Externally generated changes (e.g. changes in legislation, security threats, recommended best practice, etc)
- All users shall be informed of changes to this policy which affect them.

Declaration

I accept that I have a responsibility to safeguard Welland Park Academy information, access and equipment by abiding by the conditions of use defined in this Information Security Policy & the Acceptable Use of IT Policy.

I understand that misuse of electronic and other communications may lead to consequences, which could be harmful to individuals, the Council, the School or other organisations. I understand that for certain types of misuse, I may be open to criminal prosecution under the Obscene Publications Act, the Computer Misuse Act or the Data Protection Act.

I understand that in order to ensure that the Information Security Policy is properly followed, and to maintain the effectiveness, integrity and security of the network, the use of electronic communications will be monitored.

Name: ……

Signed: ……

Date: ……

*This declaration will be picked up by the automated forms for Acceptable Use of IT for annual sign off.