GREENWOOD ACADEMIES TRUST

IT Acceptable Use Policy

Version: 12.0 Approval Status: Approved

Document Owner:	Stephen Sanderson
Classification:	Internal
Effective From:	09/11/2021

Table of Contents

1. IT Service Desk 3
2. Key Things to Consider 3
3. Use of Email 4
4. Use of Internet 4
5. New and Departing Staff 4
6. Security and Passwords 4
7. Network and File Security and Housekeeping 5
8. Mobile Phones 5
9. Use of Laptops 6
10. Lock Screen Policy 6
11. Direct Access 6

Introduction

This document outlines the Acceptable Use Policy for Information Technology (IT) in the Greenwood Academies Trust (GAT). It also provides advice on guidance on how to use the Greenwood Academies Trust's IT effectively and gain support.

Any Employee in any doubt about, or do not understand any part of the Acceptable Use Policy, then raise this with your line manager who can then take your questions to the Trust Service Delivery Manager.

1. IT Service Desk

The Service Desk is available from 08:00-16:00, Monday to Friday and should be your first point of contact for any questions regarding the Greenwood Academies Trust IT provision.

The Service Desk is available via the following methods:

Portal: Accessible from Airhead or https://gatservicedesk.freshservice.com
Phone: 0115 748 3370 (ext 5050 if internal)
Email: servicedesk@greenwoodacademies.org

You must log all IT queries with the Service Desk. If a query is not logged, we cannot track it and ensure it meets our standards of service.

What the Service Desk **will do**:

- Support you to use GAT IT effectively.
- Resolve faults with IT equipment and services.
- Make changes to existing IT equipment and services.
- Give advice and training.
- Ensure that GAT's systems are available.
- Help scope, procure and setup new requirements.

What the Service Desk **won't do**:

- Operate applications on your behalf.
- Load paper to printers.
- Support your personal IT needs.
- Support devices that are not procured, setup and maintained by the IT Team.

Further details of the services provided by the managed service are contained within the Service Level Agreement (SLA) for your site.

2. Key Things to Consider

- Never share or write down your password.
- Do not send work documents or work data to your personal email.
- Use the GAT Email and Internet connections responsibly.

Malware, Virus and phishing attempts are ever prevalent, care must be taken not to fall foul of these.

Using a personal device to access Academy Business should be used with care, the same level of access to sensitive data can be achieved anywhere so extra care must be taken when using the system out of the office. Especially from home, remember to be aware of who else may use the device, your surroundings and to not save passwords and log out.

All assigned equipment needs to be looked after and may be requested by IT to update.

The Service Desk may refuse to install software which it cannot support or which is already met by an existing provision.

3. Use of Email

Email is often used to send viruses or malware; if you receive an unsolicited email, **do not open it or any attachments it may include**.

Do not respond to “Phishing” emails – these are created to look official, from a bank or other reputable organisation. They can contain dangerous links or claim that there has been a security breach. These links are usually directed to fake sites that collect personal information, often used to steal money or other sensitive data. You should never respond to any such requests. Reputable organisations will never ask for your details in this manner. The Greenwood Academies Trust is not responsible for any personal loss/damage caused as a result of clicking on such links.

4. Use of Internet

The Trust uses an enterprise grade system to filter and log Internet usage. As standard, certain categories of website are filtered out (such as gambling, pornography and terrorism)..

If you require access to a website for work purposes that is blocked by the filter, permission must be sought from your e-Safety Officer or Principal.

The GAT network and Internet connection must not be used for any commercial purposes other than for Trust business.

Guidance on social media and eSafety is covered in the Staff Code of Conduct and Pupil DCC.

A Trust device may be used to access none work related sites, outside of work designated hours.

5. New and Departing Staff

Your access to the GAT IT system is managed by your data administrator, supported by the Service Desk. You are not authorised to access the GAT IT system outside of your contracted dates of employment.

There is a Non-Disclosure Agreement (NDA) available for staff who require access to IT prior to their contract start date. This can be obtained via the Trust Policies site and is the responsibility of the Principal to authorise in exceptional circumstances.

6. Security and Passwords

Every staff member will be given a username and ID which gives them access to the network. These must be kept private, must not be written down or shared with anyone.

No one may use another person’s login to access information or files. If you log in using another GAT member of staff’s ID, this may be treated as misconduct and the employee(s) responsible will be dealt with as set out in GAT’s Disciplinary Policy.

If you need to share information, documents or emails with others and are unsure how to, please contact the Service Desk as there are secure ways of sharing information.

You should endeavour to use a “strong” password, containing both letters and numbers, at least one capital letter and ideally a “special character” (e.g., @!£$%&*).

You have a duty as a GAT employee to uphold and maintain high levels of data security in line with the Trust Data Protection policy. Should you be unsure or if you encounter any potential breaches of security involving you or any other staff member, you must advise the Data Protection Officer (DPO) as soon as possible.

The DPO is Alison Hope and she can be contacted by mobile on 07500 925141 or by email at dataprotection@greenwoodacadmies.org.

Details of how to report a breach are found in the appendix to the Trust Data Protection policy. It is important all staff read and have an understanding of the Data Protection policy; this will form part of the staff induction programme.

You can access the GAT system from any device from anywhere. You are responsible for ensuring that everything you access and use is kept secure. You must be mindful of your surroundings when accessing any sensitive data both at home and in public places.

GAT employees may get access to licences and software; these are also accessible on your personal device, such as a home PC or tablet. This feature is provided solely to complete tasks dictated by your GAT role.

7. Network and File Security and Housekeeping

You must not store data linked to the Academy on any device that is not supplied or approved by GAT. This includes your home PC.

All GAT files and folders are stored in the cloud (Microsoft OneDrive) and can be accessed from anywhere, on any device and can be shared among your colleagues. OneDrive also allows access from multiple countries and so there are additional security measures if using a non-Trust device from outside the UK; account security is confirmed by Multi Factor Authentication (MFA).

Document Tagging will be added to enable another level of security on shared documents. This added security will allow restrictions in sharing, printing and even includes additional access restrictions.

Care must be taken when accessing GAT documents, especially those containing sensitive data, so that access isn't granted to the wrong individual.

The use of un-encrypted USB memory sticks to transfer files is forbidden as these are insecure, not backed-up, easily lost and are a primary cause of computer viruses. Should you wish to move a document between machines, please contact the Service Desk who will explain how to use our shared groups, share files or how to encrypt a memory stick.

Malware is an application surreptitiously loaded when visiting a website. It contains code affecting the operation of the machine or threatens security through the propagation of spam email or duplicitous links (URLs), which can steal credentials and compromise data. All GAT machines are protected by anti-virus and anti-malware software. All staff should ensure that laptops are connected to the Internet and the GAT network regularly to allow updates to be made and must never cancel any pending updates. If you believe your anti-virus software is out of date, please contact the Service Desk.

You should regularly clear out and archive old documents or emails. Please ensure that you regularly empty your deleted items folder in Outlook and Recycle Bin on your computer. Please contact the IT Service Desk if you are unsure how to do this.

8. Mobile Phones

The Trust can provide mobile phones to staff whose role requires their use. All phones must be ordered through the Service Desk so that the Service Desk has a record and can set up the device on InTune. It is up to the Line Manager of the staff member to justify whether that staff member receives a mobile phone.

All mobile phones should be secured with a PIN/password. Please contact the Service Desk if you are not sure how to set this up.

9. Use of Laptops

GAT can provide laptops to staff whose role requires their use. It is up to the Line Manager of the staff member to justify whether that staff member receives a laptop.

You are responsible for your assigned laptop and you should take care to secure it.

When transporting a GAT laptop, this should always be kept in a laptop case designed for this purpose. The Service Desk will provide a quote for this if required. If this type of case is not used and a laptop is subsequently damaged as a result, GAT reserves the right to charge the staff member to cover repair or replacement costs.

You are expected to take good care of any GAT supplied IT and must return it upon demand should the Service Desk require access to it. Before leaving the organisation, staff are expected to return the laptop and all of its accessories (chargers, leads, case, etc.) in good order and without delay. GAT reserves the right to charge for any missing/damaged items not consistent with reasonable wear and tear.

10. Lock Screen Policy

A lock screen helps to protect the information displayed on your screen as well as the information that is accessible from your computer when you leave it unattended.

All computers are configured to initiate a lock screen. This security lockout feature will automatically initiate if the computer is idle for a ten-minute time period. The user must then re-enter their password to gain access to the computer.

You can initiate this manually by pressing the Windows Key and L keys simultaneously or by pressing Control-Alt-Delete and select "lock computer."

Always lock your screen when leaving the computer for any amount of time.

11. Direct Access

Trust laptops will automatically connect to the Trust network when a connection to the internet is present, this will give filtered access comparable to what will be found while working on site.

Please note:

- The connection time to make all systems available is dependent on the speed of your broadband, please allow at least two minutes for the connection to be established.
- If you are connected over wireless the connection is only made after you have successfully logged in to the computer.

12. Monitoring, Review and Evaluation

The Trust reserves the right to withdraw or suspend a user's access to the system should the Trust deem the staff member to be in breach of the Trust's policies and procedures.

The Trust IT Acceptable Use Policy and other associated policies and procedures are reviewed every two years or sooner, if required, due to a change in legislation. Trust policies and procedures are approved by Trustees and are subject to Trade's Union consultation.

User guides, help articles and videos are available and all users should familiarise themselves with these guides. Should further training be required, please contact the Service Desk.