Ascend Learning Trust

Acceptable Use Agreement 2022-23

This Technology user agreement applies to all employees, future employees, supply staff, visitors, volunteers and contractors.

Written by:	A collaboration of members from the Safeguarding Leads, IT Leads, the Executive Team and DPO
Date Ratified by ALT:	10th May 2023
Version number:	1
Committee Reviewed:	ALT Trustees
Document Type:	Tier 2 Template
Date ratified by LGB:	November 2023
Adopted by:	Royal Wootton Bassett Academy
Related policies:	Online Safety Policy
Review date:	Annually

Contents

Quick Reference Contacts Guide

	Name	Contact Details
Designated Safeguarding Lead (DSL)	Mari Roberts	mroberts@rwba.org.uk 01793 841928
Head teacher / Principal	Anita Ellis	aellis@rwba.org.uk 01793 841900
Deputy DSL	Mrs A Ellis Mrs K Heaphy Mrs K Salmon Mrs S McMullin	aellis@rwba.org.uk / 01793 841900 kheaphy@rwba.org.uk / 01793 841967 ksalmon@rwba.org.uk / 01793 841960 smcmullin@rwba.org.uk / 01793 841919
Designated Information Technology Lead (DITL) for the school	Z Ishani	zishani@rwba.org.uk / 01793 841900
Data Protection Officer (DPO) contact details		Email: dpo@dataprotection.education

Statement of intent

Royal Wootton Bassett Academy promote the use of technology and understand the positive effects it can have, we must also ensure that technology is used appropriately. Any individual found to have violated this agreement may be subject to disciplinary action, up to and including termination of employment.

This agreement applies to the use of Ascend Learning Trust IT systems regardless of location.

This acceptable use agreement is designed to outline the individuals responsibilities when using technology, whether this is via personal devices or school devices, or on/off the school premises, and applies to all employees, future employees, supply staff, volunteers, contractors, and visitors.

These rules are in place to protect both the school and the employee, future employee, supply staff, volunteers, contractors, or visitors, because inappropriate of the internet and our IT network and systems exposes all to unnecessary risk.

Introduction

This agreement applies to all employees (including future employees who have accepted a role at any one of the school's within the Ascend Learning Trust, volunteers, supply staff, visitors and contractors using school or trust IT facilities.

The acceptable use agreement is divided into the following three sections.

- General agreement and code of practice
- Internet agreement and code of practice
- Email agreement and code of practice

This agreement should be read in conjunction with the Ascend Learning Trust Data Protection Policy, Privacy Notice and Online Safety Policy.

The school understands that technology, the internet, and social media are powerful tools which provide opportunities for teaching and learning. This agreement ensures that all users stay safe whilst using these technologies.

General agreement and code of practice

This agreement relates to all use of technologies including mobile phones, tablets, and online services such as social networking sites provided or leased by Ascend Learning Trust

This agreement also applies to services used by Ascend Learning Trust accessed from personal devices.

This agreement sets out the rules that you must comply with to ensure that the system works effectively for everyone.

The UK GDPR and Data Protection Act 2018 require all personal and special category data to be processed confidentially, with credibility, integrity, and accuracy. This applies to all data the school, Trust, its organisations and departments stores and processes on its network.

Privacy

Whilst the school and Ascend Learning Trust seeks to provide a reasonable level of privacy, users should be aware that the data they create on the various networks and systems remain the property of Ascend Learning Trust.

The school, Trust, organisations and its departments will only process data in line with its lawful basis to uphold the rights of all data subjects.

In order to protect individuals safety and wellbeing, and to protect the Trust from any third party claims or legal action against it, authorised individuals within the Trust or any individual school may view any data, information, or material on the IT systems and networks (whether contained in an email, call recordings, on the network, notebooks, or laptops) and in certain circumstances, determined by the Data Protection Officer, disclose that data, information, or material to third parties, such as the police or social services if required. The Ascend Learning Trust Privacy Policy details the lawful basis under which the school is lawfully allowed to do so.

When users are allocated a Trust or school email address, the relevant IT department will automatically provide users with a standardised email signature disclaimer stating: "*The contents of this message do not necessarily represent the opinions, views, policy or procedures of* Royal Wootton Bassett Academy. *This message is private and confidential. If you have received this message in error, please notify us and remove it from your system. If you are not the intended recipient of this email, you must neither take any action based upon its contents, nor copy or show it to anyone. Please note that* Royal Wootton Bassett Academy *does not warrant that any attachments are free from viruses or other defects and accepts no liability for any losses resulting from infected email transmissions."* This signature must not be removed or changed in any way and will be attached to all emails whether those emails are outbound or forwarded.

Code of practice

The Trust's philosophy	In using IT, you will follow the Trust 's ethos and consider the work and feelings of others. You must not use the system in a way that might cause annoyance or loss of service to other users.
Times of access	With the implementation of Microsoft 365 across the Trust, users with the appropriate levels of authority can access the school network at all times using the appropriate browser. This acceptable use agreement applies at all times and in all places on all devices.
Use of Microsoft 365 or any other browser-based platform that allows access to the personal, confidential, or financial information of data subjects	These platforms include but are not limited to, the following platforms: Microsoft Teams, SharePoint, One Drive, Outlook, CPOMS, SIMS/Arbor, Provision Insight Tracker Map etc. Each individual school will enforce the most appropriate authentication for access to each of these platforms. Moving forward it is likely that Multi Factor Authentication will be mandated for all staff for all platforms.
User ID and password and logging on	You will be given your own personal and confidential user ID and password, which will allow you to access the network and associated platforms. You must keep these private and not share them with anyone and you may not use any other individual's ID or password to login to any systems or cloud-based platforms The facilities are allocated to you on a personal basis, and you are responsible for the use of any device when you are logged on. Be aware that all user areas on the Trust and school network and all communication channels are monitored to maintain system integrity. If you forget or accidentally disclose your username and password to anyone else, you must report it immediately to a member of the IT support staff who will change your credentials.

	Use of the school's facilities by a third party using your username or password will be attributable to you, and you will be held accountable for the misuse.
Access to information not normally available	You must not use the Trust or school IT systems or the internet to find or use facilities or flaws in the system that might give access to information or areas of the network not normally available to you. You must not attempt to install software to explore or harm the system. Use of hacking tools, e.g. 'loggers', 'sniffers' or 'evidence elimination software', is expressly forbidden.
Downloading of information from any Trust or school network to personal devices for personal use	You must not download information, including personal information and teaching and learning resources to any personal device for your own benefit. School and Trust networks are monitored for unusual or excessive activity and will investigate individual usage if notified or identified.
Images and videos	To prevent allegations of inappropriate activities, including against staff, you must not store images of pupils on any personal device. Any images taken on personal devices must be downloaded to the school network as soon as reasonably possible and deleted from any and all personal devices.
Communicating with staff and students	To protect both students and staff, you must only communicate using your allocated email address, work phone or other school communication system. You must not use personal phones, email, or social media unless in an emergency.
Connections to the system	You must not connect any hardware which may be detrimental to the school's network.
Connections to the computer	You must not adjust or alter any settings on any of your school devices without first obtaining the explicit written permission of a member of the IT staff. You are not permitted to connect anything else to your device or download external third-party software without first getting the explicit written permission of a member of the IT staff.

Virus	If you suspect that your computer has a virus, you must report it to a member of the IT staff immediately.
Installation of software, files, or media	You must not install or attempt to install software of any kind on the school network drives or local hard drives of networked desktop computers, laptops, or tablets. You must not alter or re-configure software on any part of the school's system.
File space	You must manage your own file space by deleting old data rigorously and by deleting emails, documents, or images that you no longer require. If you are unsure of the retention period for each type of data please consult the Trust retention schedule or contact the data protection officer (DPO). If you believe that you have a real need for additional space, please discuss this with a senior member of the IT support staff.
Reporting faults and malfunctions	You must report any faults or malfunctions in writing to the IT support staff, including full details and all error messages, as soon as possible.
Copying and plagiarising	You must not plagiarise or copy any material which does not belong to you.

Internet agreement and code of practice

The school and the Trust provides access to the internet from within the relevant locations. This access is actively filtered to remove any inappropriate access to banned sites and to protect the network from external attack.

Whenever accessing the internet using the school's, the Trust's or personal equipment you must observe the code of practice below.

This agreement and code of practice is designed to reduce and control the risk of offences being committed, liabilities being incurred, employees or students being offended and the school's facilities and information being damaged.

Any breach of this agreement and the code of practice will be treated extremely seriously, and it may result in disciplinary or legal action or expulsion.

The school may take steps, including legal action where appropriate, to recover from an individual any expenses or liabilities the school incurs because of the breach of this agreement and code of practice.

Why is internet access available?

The internet is a large and invaluable source of information. Numerous websites and services, both official and unofficial, provide information or links to information which would be useful for educational purposes.

Why is a code of practice necessary?

There are four key issues:

- Although the internet is often described as 'free', there is a significant cost to the school for using it. This cost includes the computer hardware, software and resources needed to support internet access.
- Although there is much useful information on the internet, there is a great deal more material which is misleading, irrelevant or detrimental.
- Unfortunately, the internet carries a great deal of unsuitable and offensive material. It is important for legal reasons, reasons of principle, and to protect all employees of the school and Trust, and students who access the internet, that it is properly managed. Accessing certain websites and services, and viewing, copying, or changing certain material, could amount to a criminal offence and give rise to legal liabilities.
- There is a danger of importing viruses on to the school's network, or passing viruses to a third party, via material downloaded from or received via the internet, or brought into the school on disks or other storage media.

Code of practice

Use of the internet	The Internet should not normally be used for private or leisure purposes; it is provided primarily for education or business use. You may use the internet for other purposes provided that: • Such use is occasional and reasonable; • Such use does not interfere in any way with your duties; and • You always follow the code of practice.
Inappropriate material	You must not use the internet to access any newsgroups, links, list-servers, web pages or other areas of cyberspace that could be offensive because of pornographic, indecent, racist, violent, illegal, illicit, or other inappropriate content. "Inappropriate" in this context includes material which is unsuitable for viewing by students. You are responsible for rejecting any links to such material which may appear inadvertently during research. If you encounter any material which could be regarded as offensive you must leave that website or service immediately and not make any copy of that material. If you encounter any difficulty in leaving a website or service, you must inform the IT support staff immediately.
Misuse, abuse, and access restrictions	You must not misuse or abuse any website or service or attempt to bypass any access controls or restrictions on any website or service.
Monitoring	The internet access system used by the school maintains a record which identifies who uses the facilities and the use that you make of them. The information collected includes which website and services you visit, how long you remain there and which material you view. This information will be analysed and retained, and it may be used in disciplinary and legal proceedings.
Giving out information	You must not give any information concerning the school, its pupils or parents, or any employee when accessing any website or service. This prohibition covers the giving of names of any of these individuals – the only exception being the use of the school's name and your name when accessing a service which the school subscribes to.

Hardware and software	You must not make any changes to any of the school's hardware or software. This prohibition also covers changes to any of the browser settings. The settings put in place by the school and the Trust are an important part of the security arrangements and making any changes, however innocuous they might seem, could allow hackers and computer viruses to access or damage the school's systems.
Copyright	You should assume that all material on the internet is protected by copyright and must be treated appropriately and in accordance with the owner's rights. You must not copy, download, or plagiarise material on the internet unless the owner of the website expressly permits you to do so.

Email agreement and code of practice

The school's computer system enables members of the school and Trust to communicate by email with any individual or organisation with email facilities throughout the world.

For the reason outlined above, it is essential that a written agreement and code of practice exists, which sets out the rules and principles for use of email by all.

Any breach of this agreement and code of practice will be treated seriously and it may result in disciplinary or legal action or expulsion.

The school may take steps, including legal action where appropriate, to recover from an individual any expenses or liabilities the school incurs because of the breach of this agreement and code of practice.

Code of practice

Purpose	You should only use the school's email system for work related emails.
Trust's email disclaimer	The school's email disclaimer is automatically attached to all emails by the IT department regardless of whether they are outgoing emails or forwarded emails, you must not cancel or disapply it.
Monitoring	Copies of all incoming and outgoing emails, together with details of their destination are stored on the network (in electronic form). The frequency and content of incoming and outgoing external emails may be checked to determine whether the email system is being used in accordance with this agreement and code of practice. Certain authorised individuals within the school and the Trust are entitled to have full access to your emails.
Security	As with anything else sent over the internet, emails are not completely secure. There is no proof of receipt, emails can be 'lost', they can suffer from computer failure and a determined 'hacker' could intercept, read, and possibly alter the contents. As with other methods of written communication, you must make a judgment about the potential damage if the communication is lost or intercepted. Never send sensitive personal information, bank account information, including passwords, by email unless they are password protected.

Program files and non-business documents	You must not introduce program files or non-business documents from external sources onto the school's network. This might happen by opening an email attachment or by downloading a file from a website. Although virus detection software is installed, it can never be guaranteed 100 percent successful, so introducing nonessential software is an unacceptable risk for the school. If you have any reason for suspecting that a virus may have entered the school's system, you must contact the IT support staff immediately.
Quality	Emails constitute records of the school and are subject to the same rules, care and checks as other written communications sent by the school. Emails may be checked under the same scrutiny as other written communications. Employees should consider the following when sending emails: • Whether it is appropriate for material to be sent to third parties. • The emails sent and received may have to be disclosed in legal proceedings. • The emails sent and received may have to be disclosed as part of fulfilling a Subject Access Request. • Whether any authorisation is required before sending. • Printed copies of emails should be retained in the same way as other correspondence, e.g. letter. • Confidentiality between sender and recipient. • Transmitting the work of other people, without their permission, may infringe copyright laws. • The sending and storing of messages or attachments containing statements which could be construed as abusive, libelous, and inappropriate may result in disciplinary or legal action being taken. • Sending or storing messages or attachments containing statements which could be construed as improper, abusive, harassing the recipient, libelous, malicious, threatening, or contravening discrimination legislation or detrimental to the school or Trust is a disciplinary offence and may also be a legal offence.

Inappropriate emails or attachments	You must not use email to access or send offensive material, chain messages or list-servers or for the purposes of bullying or plagiarising work. You must not send personal or inappropriate information by email about yourself, other members of staff, pupils, or other members of the school community. If you receive any inappropriate emails or attachments, you must report them to IT support team.
Viruses	If you suspect that an email has a virus attached to it, you must inform the IT support team immediately.
Storage	Old emails may be deleted or archived from the school's server after 12 months. You are advised to regularly delete material you no longer require and to archive material that you wish to keep as long as you have a reason to do so. For further information please see our Records Retention Policy or contact the data protection officer for advice.
Message size	Employees are limited to sending messages with attachments which are over a certain size. If you wish to distribute files within the school, you can do so by using shared areas such as SharePoint or One Drive.
Confidential Emails	You must ensure that confidential emails are always suitably protected. If working at home or remotely, you should be aware of the potential for an unauthorised third party to be privy to the content of the email. Confidential emails should be deleted when no longer required.

Email agreement – advice to employees

- Employees should remind themselves of the Online Safety Policy which relates to the monitoring and security of emails. In addition, employees should be guided by the following good practice:
- Employees should check their emails daily and respond, as appropriate, within a reasonable period if the email is directly addressed to them.
- Employees should avoid spam, as outlined in this agreement.
- Employees should avoid using the email system as a message board and thus avoid sending trivial global messages.
- Whilst accepting the convenience of the staff distribution list, employees should try to restrict its use to important or urgent matters.

- Employees should send emails to the minimum number of recipients.
- Employees should always include a subject line in emails.
- Employees are advised to keep old emails for the minimum time necessary.

Further guidelines

- Remember – emails remain a written record and can be forwarded to others or printed for formal use.
- As a rule of thumb, employees should be well advised to only write what they would say in an official work related letter or face to face and should avoid the temptation to respond to an incident or message by email in an uncharacteristic and potentially aggressive fashion.
- Remember, "tone" can be misinterpreted on the printed page and once it is sent it could end up in the public domain forever. Email lacks the other cues and clues that convey the sense in which what you say is to be taken, and you can easily convey the wrong impression.
- Remember that sending emails from your school account is similar to sending a letter on school letterhead, so don't say anything that might bring discredit or embarrassment to yourself or the school.
- Linked with this and given the popularity and simplicity for recording both visual and audio material, employees are advised to remember the possibility of being recorded in all that they say or do.

For further information or to clarify any of the points raised in this agreement please speak to your IT support team or Data Protection Officer.

Please sign below to confirm you have read and understood the Trust Technology Acceptable Use Agreement:

Signed on behalf of school: _____

Print name & Position: _____

Name of school: _____

Date: _____

Signed by employee / future employee / supply teacher / volunteer / contractor / visitor:

Signature: _____

Print name & Position: _____

Name of school: _____

Date: _____

I understand a copy of this signed document will be placed on my personal file.