Acceptable Use Policy

This policy is applicable to the Wonder Learning Partnership (WLP)

Important: This document can only be considered valid when viewed on the Wonder Learning Partnership website. If this document has been printed or saved to another location, you must check that the version date on your copy matches that of the document online.

Version Approved: June 2026

Chief Executive Officer (CEO) Approved:	Summer Term 2026
Name of Responsible Committee/Individual:	Board of Trustees
Implementation Date:	Summer Term 2026
Review Date:	Summer Term 2029

Contents

Introduction and Scope

The Acceptable Use policy includes accessing applications and cloud services on personal devices and governs the use of Wonder Learning Partnership devices, corporate network and cloud-based systems that individuals use on a daily basis in order to carry out business functions or either a personal or work phone.

This policy applies to all employees, governors or trustees, contractors, agents and representatives, volunteers and temporary staff working for, or on behalf of, the school.

This policy should be read in conjunction with the other policies in our information governance policy framework, including the Data Protection policy, Information Security policy and Records Management policy.

It should be noted, every employee has access to a Trust device, a laptop or desktop and some mobile phones. Telephone calls and data management can be facilitated through a laptop.

Email and Internet Use

We provide email accounts and internet access to the workforce to assist with performance of their duties. We also allow the workforce to use its instant messaging service. For the benefit of doubt Instant Messages are classed as email communications in this policy.

Personal Use

Whilst text messaging, email accounts and the internet should primarily be used for business functions, incidental and occasional use in a personal capacity may be permitted so long as:

- Personal messages or internet usage do not tarnish our reputation, or infringe on business functions,
- Users understand that text messages, emails sent to in relation to Trust, educational partners and from corporate accounts are the property of the school or Trust,
- Users understand that we may have access to their text, email account and any personal messages contained within,
- Users understand that we may have access to their social messaging ontent, internet browsers and browsing history contained within,
- Users understand that texts and emails sent to or from an employee, a partner to the Trust or an individual in the sector, may have to be disclosed under Freedom of Information and/or Data Protection legislation,
- Users understand that we reserve the right to cleanse email accounts at regular intervals which could result in personal emails being erased from the corporate network,
- Users understand that we reserve the right to suspend phone or internet access at any time.

Inappropriate Use

We do not permit individuals to send, forward, or solicit texts or emails, or use the internet in any way that may be interpreted as insulting, disruptive, or offensive by any other

individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit or pornographic messages, images, cartoons, jokes, or movie files,
- Unwelcome propositions, profanity, obscenity, slander, or libel,
- Any messages or content containing ethnic, religious, political, or racial slurs,
- Any messages or content that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

Users are also not permitted to use the internet in a way which could affect usage for others. This means not streaming or downloading media files and not using the internet for playing online games.

Other Business Use

Users are not permitted to use texts or emails or the internet to carry out their own business or business of others. This includes, but is not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case-by-case basis at the discretion of school or Trust management.

Security

Users will take care to use their email accounts and the internet in accordance with our Information Security policy. In particular users will:

- Not click on links from un-trusted or unverified sources,
- Use secure email transmission methods when sending personal data,
- Not sign up to marketing material that could jeopardise our IT network,
- Not send excessively large email attachments without authorisation from management and our IT provider.

Group Email Accounts

Users may also be permitted access to send and receive emails from group and/or generic email accounts. These group email accounts must not be used in a personal capacity, and users must ensure that they sign each email with their name so that emails can be traced to individuals. Improper use of group email accounts could lead to suspension of a user's email rights.

The Trust Chief Operating Officer will have overall responsibility for allowing access to group email accounts, but this responsibility may be devolved to other individuals.

We may monitor and review all email traffic that comes to and from individual and group email accounts.

Social Media Use

We recognise and embrace the benefits and opportunities that social media can contribute to an organisation. We also recognise that the use of social media is a data protection risk due to its open nature and capacity to broadcast to a large amount of people in a short amount of time.

Corporate Accounts

We have a number of social media accounts across multiple platforms. Nominated users will have access to these accounts and are permitted to post general information about the school and/or Trust. Authorised users will be given the usernames and passwords to these accounts which must not be disclosed to any other individual within or external to the organisation. The Director of Estates and Compliance will have overall responsibility for allowing access to social media accounts.

Corporate social media accounts must not be used for the dissemination of personal data either in an open forum or by direct message. This would be a contravention of our information governance policies and data protection legislation.

Corporate accounts must not be used in a way which could:

- Tarnish our reputation,
- Be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs,
- Be construed as sexually explicit,
- Be construed as political beliefs or commentary.

Personal Accounts

We understand that many users will use or have access to personal social media accounts. Users must not use these accounts:

- During working hours,
- Reference of speak on behalf of their employer, Trust or school.
- Using corporate equipment,
- To conduct corporate business,
- To contact or approach our clients, customers, or partners.

Telephone and Video Conferencing Use

We provide users with access to telephone and video conferencing services to assist with performance of their duties.

Personal Use

Whilst telephone and video conferencing services should primarily be used for business functions, incidental and occasional use in a personal capacity may be permitted so long as:

- Usage does not tarnish our reputation or infringe on business functions,
- Users understand that we may have access to call history and recordings,
- Users understand that we reserve the right to suspend telephone and video conferencing usage at any time,
- Telephone call or video conference recordings or transcripts may have to be disclosed under Freedom of Information and/or Data Protection legislation.

Inappropriate Use

We do not permit users to use the telephone or video conferencing services in any way which may be interpreted as insulting, disruptive, or offensive by any other individual or entity.

Other Business Use
Users are not permitted to use these services to carry out their own business or business of others. This includes work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case-by-case basis at the discretion of school or Trust management.

Appendix One – Accessing cloud services on personal devices

Introduction
As remote working continues to develop, there has been a move by many organisations to transfer their locally held data into the cloud, enabling access by any internet connected device, anywhere in the world. This brings many benefits to the school, including being able to access data promptly. Personal devices are not permitted for business use. The Trust will provide all teaching and other selected staff with a device to be used for all business functions both in and out of Trust premises.

However, with this enhanced access and benefits comes a high level of risk that the school needs to consider and mitigate through the use of technical controls, expected behaviours and supporting policies. This policy aims to provide the framework for adequate management of the risks posed when users access school systems..

Permitted Activity
Whilst using devices outside Trust premises, users are permitted to access, review and process personal data within the school system in which it is held. Users must only access data they are entitled to in order to fulfil their duties.

It is not permitted for any school data, including text or emails, to be downloaded and saved onto any personal device under any circumstances without the approval of the Chief Operating Officer and the installation of Comp Portal. All school data must remain within the defined systems to ensure it remains secure, available to all authorised personnel and held within our records management system for its full lifecycle, including secure destruction in line with our retention schedule.

By retaining data within school-controlled systems, in the event of an individual exercising their rights as detailed in the UK GDPR; particularly with the right to access (Subject Access Request), the searching criteria to meet a request will not require users to search their own devices for evidence of personal data that may have been stored.

Printing of any personal data to home printers is strictly forbidden. The storage and confidential disposal of paper documents cannot be easily managed and guaranteed when taken off the school site.

Device Security

Anti-virus and software security patching
Anti-virus and software security patching, along with software updates, will be centrally managed through cloud deployment by a certified external service provider. Staff should not try installing any software on Trust owned devices . Requests should be directed in writing to the Trust's Chief Operating Officer or Director of Technology Service and Dasta.

Password/PIN protection
All devices are secured by a unique password to ensure that access to the device is limited to the named user permitted to access the school's personal data.

Equipment disposal
The Trust is responsible for the disposal of non-functioning or obsolete devices. These should be returned to the Schools' Head Teacher or Trust Head Office where a Returned Device Form must be completed and retained electronically with the relevant department.

Physical security
Users should ensure any device used to access school data is kept safe and secured to prevent theft or damage. This includes actions such as not leaving devices overnight in cars, unattended in public spaces, or transported without sufficient protection to prevent accidental damage.

System and Accounts Security
When accessing data held in the cloud via an internet connection (e.g. Microsoft 365), users must ensure that their account is closed when not in use by logging out of the system. It is not permitted for accounts to be left open when not in use, if accessing school systems.

Users are responsible for ensuring any internet connection used to access school data is secured through the use of access controls, such as using a designated username and password. Unsecured network connections (Wi-Fi or hot spots) must not be used, and devices Will be configured to prevent automatic connection to unknown networks (e.g. cafes, shopping centres, library etc.).

Data Breaches

In the event of a data breach users must follow the process detailed in the Information Security policy and report any suspected breach immediately.

Users are asked to be mindful of the following situations in which the risk of a data breach increases:

- Systems are not shut down appropriately when not in use, leading to unauthorised access of school data.
- Trust devices are shared with family, friends, or partners leading to unauthorised access of school data.
- Documents and files are downloaded onto shared devices and then become accessible to other users of the device.

- Passwords or security PINs are shared with others (e.g. family and partners) leading to unauthorised access of school data.
- Disposal of devices has not followed the policy of return to the nominated Trust representative.

Authorised Access

Access to school systems using personal devices is not permitted In the event that the user leaves the employment of the school; or the relationship terminates for third parties and contractors; access should not be attempted and all devices must be returned to the nominated Trust representative. Any attempt to later access data would be treated as a data breach and investigated as such.

It is a criminal offence under Section 170 of the Data Protection Act 2018 to knowingly access data that you are not entitled to or after you have left our employment.

Exemption Process

An exemption to any element of this policy can only be authorised by the Cheif Operation Officer. Authorisation will only be given where there is a clear business need and following a full risk assessment to ensure risks are mitigated.