PONTEFRACT
ACADEMIES TRUST

Acceptable Use Policy – Workforce

Summary:
This policy sets guidelines and rules on the use of ICT resources for all employees, SPRB members, Trustees, contractors, agents and representatives, volunteers and temporary staff working for, or on behalf of, the Trust.

Author	Lead Governance Officer		
Applies to: (please check as appropriate)	Staff ✓	Pupil	Community
Ratifying Committee(s):	Education and Standards Committee		
Available on:	Compliance Library ✓	Website ✓	
Date of Approval:	04/07/2025		
Date of Next Formal Review: (ensure this is aligned to committee meeting dates)	02/07/2026		
Review Period:	Annual		
Status:	Non-statutory		
Owner:	**Pontefract Academies Trust**		
Version:	1.0		

Document Control

Date	Version	Action	Amendments
February 2025	1.0	New policy	New workforce policy based on Veritau model

Contents

1. Introduction and scope

The Acceptable Use Policy – Workforce governs the use of Pontefract Academy Trust's corporate network and cloud-based systems which individuals use daily to carry out business functions.

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 and Data Breach Recovery Policy, Information Security policy and Records Management policy.

2. 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.

Employees should enable multi-factor authentication on their email accounts. All work-related business should be conducted using the email address provided by the Trust. Employees must not share their personal email addresses with parents and pupils and must not send any work-related materials using their personal email account.

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Personal Use

Whilst 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:

- Such use does not take place during contact time/teaching hours/non-break time.
- Usage does not constitute 'unacceptable use'
- Usage takes place when no pupils are present
- Usage does not interfere with their jobs or prevent other staff or pupils from using the facilities for work or educational purposes
- Personal messages or internet usage do not tarnish our reputation, or infringe on business functions
- Users understand that emails sent to and from corporate accounts are the property of the school or Trust
- Users understand that we may have access to their email account and any personal messages
- Users understand that we may have access to their internet browsers and browsing history
- Users understand that emails sent to or from their email account 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 internet access at any time

Inappropriate Use

We do not permit individuals to send, forward, or solicit 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.

Users who engage in inappropriate use may face disciplinary action in line with the Trust's Behaviour Policy, Disciplinary Policy or Code of Conduct.

Other Business Use

Users are not permitted to use 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 Trust management.

Security

Users will take care to use their email accounts and the internet in accordance with our Information Security policy. 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 Information Asset Owner 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 to and from individual and group email accounts.

3. 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 several 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 Information Asset Owner will have overall responsibility for allowing access to social media accounts. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

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
- Using corporate equipment
- To conduct corporate business
- To contact or approach our clients, customers, or partners

Request for comment through social media

If you are contacted for comment about the Trust for publication anywhere, including in any social media or news outlet, direct the enquiry to the Marketing and Communications Manager and do not respond without written approval.

Recruitment and social media

In line with Keeping Children Safe in Education statutory guidance, schools should consider carrying out an online search as part of their due diligence, during recruitment shortlisting processes. This may help identify any incidents or issues which have occurred and are publicly available online, which the recruiting manager may want to explore with the applicant during the interview process.

Responsible use of social media

The following section of this policy provides staff with common sense guidelines and recommendations for using social media responsibly and safely. They apply to both personal and Trust-affiliated accounts.

Safeguarding children and young people

- You must not communicate with students over social media sites.
- You must never send a direct message to a student through a social media account.
- Staff must not respond to any direct communication from a student.
- Students' personal accounts should never be tagged in a social media post.
- Staff must not accept any current student of any age as a follower on a personal account.
- Any communication received on a personal account from a student must be reported to the Designated Safeguarding Lead in school.
- If a social media platform is being used as a way for students to collaborate with a member of staff as part of a school project or specific subject, that account must be made private.
- You must block unwanted communications from students.
- You should not interact with any ex-student of the Trust who is under 18.
- Privacy settings should be set so that age restrictions are set at 13+. Children under 13 are not legally allowed to create social media accounts.
- You should enable a profanity filter.
- Any sharing of links to external sites must be appropriate.
- Abusive or threatening posts should be reported to your manager and the Marketing and Communications Manager.
- Avoid posting anything on a personal account that you do not want your students to see and consider stricter privacy settings.
- Only use Trust owned equipment to post to a Trust social media account.

Protecting our reputation

- Staff must not post disparaging or defamatory statements about the Trust, students, parents or carers, trustees, staff, suppliers or any other Trust stakeholders.
- Staff should avoid posting messages that might be misconstrued in a way that could damage our reputation.
- If you disclose your affiliation as an employee of our Trust on a personal account (this can include simply interacting with Trust accounts such as liking/sharing etc), you must also state that your views do not represent those of your employer. Please add in your bio – views are my own.
- You should ensure that your profile and any content you post are consistent with the professional image you wish to present to students and colleagues.
- Avoid posting comments about sensitive Trust-related topics.
- If you are contacted for comment about the Trust by the press or some other external agency, direct the enquiry to the Marketing and Communications Manager and do not respond without approval.
- Deal with any complaints by offering dialogue through a more appropriate channel. Direct message the complainant with alternative contact details to avoid any awkward public conversations.

Respecting intellectual property and confidential information

- Remember that anything shared through social media is subject to copyright, data protection and freedom of information legislation.

- Staff must not post anything that could jeopardise our confidential information and intellectual property.
- Staff should avoid misappropriating or infringing the intellectual property of other companies and individuals.
- Do not use our logos, brand names, slogans or other trademarks or post any of our confidential or proprietary information without prior written permission.
- Passwords should always be stored safely and should be strong. Passwords for Trust affiliated accounts should always be shared with the Marketing and Communications Manager.
- Always ensure that you log out of the Twitter account.

Respecting colleagues, students, parents and carers, trustees and other stakeholders

- Do not post anything that your colleagues or our pupils, parents and carers, trustees and other stakeholders may find offensive.
- Do not post anything related to your colleagues, our students, parents and carers, trustees, and other stakeholders without their written permission.
- Circulating chain letters or other spam is never permitted.
- Circulating or posting commercial, personal, religious or political solicitations or promotion of outside organisations unrelated to the Trust's business are prohibited.

Social media rules for staff are detailed within Appendix B.

4. Telephone and video conferencing use

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

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business. Mobile telephones should be secured with a suitable PIN or Passcode.

The use of WhatsApp for Trust purposes is strictly prohibited.

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 provided such use:

- Does not take place during contact time/teaching hours/non-break time.
- Does not constitute 'unacceptable use'.
- Takes place when no pupils are present.
- Does not interfere with their jobs or prevent other staff or pupils from using the facilities for work or educational purposes.
- 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
- Phone calls to international and premium rate numbers are always unacceptable, unless specifically required for your professional duties

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 Trust management.

Appendix A: Accessing cloud services on personal devices

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, including being able to access data promptly, individuals can use a device of their own choice, and making financial savings as we do not have to provide our own devices to users.

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 should users access school systems through a non-school provided device.

Personal Devices

We identify a personal device as any electronic device that has not been provided by us and can be used to access and process personal data, including data accessed from the cloud through an internet connection. This includes, but it not limited to:

- Laptop or PC
- Notebook
- iPad or tablet
- Smartphone

Use of the device must be limited to the individual user and not be shared resources (e.g. a family device).

Permitted Activity

Whilst using their own devices, 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 fulfil their duties.

It is not permitted for any school data to be downloaded and saved onto any personal device under any circumstances. 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

The range of devices currently available all present different levels of ability to apply appropriate security and protection to the equipment. It is therefore the responsibility of the user to ensure that all available protection and security is applied. Specialist advice should be sought where appropriate.

We require that any device used for accessing school systems in the cloud must have adequate anti-virus software. The software should be installed, configured and maintained by a suitably qualified or experienced person. All available updates must be applied in a timely manner.

Out of date software (including operating systems) can provide vulnerabilities that can be exploited by unscrupulous hackers. All software installed on devices that is going to be used to access school data must be operating at the most up to date version with all security releases applied. All software should be configured and maintained by a suitably qualified or experienced person for the full period that they are used to access school data.

Password/PIN protection

All devices must be secured by a unique password or security pin to ensure that access to the device is limited to the named user permitted to access the school's personal data. Devices that lack the ability to enforce this level of security must not be used to access school data.

Data on personal devices is unlikely to be encrypted, and therefore particularly vulnerable if lost or stolen. Having a robust password or PIN in place provides an additional layer of protection.

Personal applications (apps)

Users are asked to be mindful of the apps installed on personal devices that are used to access school data. Some of these apps may have enhanced privileges and tracking within them that monitor use of the device and other items that are being accessed. This should be detailed in the application's terms and conditions and the user should seek assurance that this risk is being effectively managed.

Equipment disposal

When a device being used to access school information is disposed of, it is the responsibility of the user to ensure that no records or school data have found their way onto the device, either accidently or for a temporary purpose, prior to surrendering it as a part of an upgrade process, at point of resell or for permanent disposal through the WEEE (Waste Electronic and Electrical) process. Specialist advice should be sought where appropriate.

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, 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 must 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 Data Protection and Data Breach Recovery 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.
- Personal 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.
- Inadequate management of security and software updates leaves a vulnerability to a virus or hack. Once unauthorised control of a device is established it is difficult to identify and remove.
- Disposal of devices that have not been adequately assessed and the permanent removal of any school related data prior to surrender.
- Sharing personal information on platforms such as generative AI tools.

Authorised Access

Access to school systems using personal devices is only permitted whilst the user has authorisation to do so. If the user leaves the employment of the school; or the relationship terminates for third parties and contractors; access should not be attempted. To do so 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 school's Senior Information Risk Owner (SIRO). Authorisation will only be given where there is a clear business need and following a full risk assessment to ensure risks are mitigated.

Appendix B: Social media rules for staff

10 social media rules for school staff

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead.
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional.
3. Check your privacy settings regularly.
4. Be careful about tagging other staff members in images or posts.
5. Don't share anything publicly that you wouldn't be happy showing to pupils.
6. Don't use social media sites during working/school hours.
7. Don't make comments about your job, your colleagues, or school or your pupils online.
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event).
9. Don't link your work email address to your social media accounts. Anyone who has this address, your personal email address or mobile number is able to find you using this information.
10. Consider uninstalling social media apps from your phone. Apps recognise Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connections, such as parents or pupils.

Check your privacy settings

- Change the visibility of your posts and photos to 'Friends only', rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list.
- Don't forget to check your old posts and photos.
- The public may still be able to see posts you've 'liked', even if your profile settings are private, because this depends on the privacy settings of the original poster.
- Google your name to see what information about you is visible to the public.
- Prevent search engines from indexing your profile so that people can't search for you by name.
- Remember that some information is always public; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender.

What to do if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile.
- Check your privacy settings again and consider changing your display name or profile picture.
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify the headteacher and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages.
- Notify the Headteacher about what is happening.

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:

- Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school.
- Pupils may have indirect access through their parent's account to anything you post, share, comment on or are tagged in.

If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so.

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way.
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred.
- Report the material to Facebook or the relevant social network and ask them to remove it.
- If the perpetrator is a current pupil or staff member, our disciplinary and behaviour policies are usually sufficient to deal with online incidents.
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material.
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime you or a senior leader should consider contacting the police.