Acceptable use Policy

Policy type	Non-Statutory
Author	Steven Bentley
Last updated	June 2025
Reviewed	Data Protection Officer
Approved by	Chief Executive Officer
Release date	August 2026
Review cycle	Every two years. Policies will be reviewed in line with Grace Schools's internal policy schedule

1. Application of this Statement

This Policy and any associated procedures, guidance, templates and training, apply to the Trust Board of Grace Schools ("Grace Schools" or the "Trust"), senior leadership team members, Central Leadership Team, Headteachers, volunteers, contractors, and any individual granted ICT access by the Trust (collectively "Staff and Agents").

This policy sets out the expectations for staff when using Trust IT systems, devices, accounts, data, communication tools, and AI platforms.

It supports safeguarding, data protection, cyber security, and the professional standards required across all Grace schools.

2. Legal & Regulatory Framework

Staff and Agents must comply with UK GDPR, the Data Protection Act 2018, Keeping Children Safe in Education, DfE Filtering & Monitoring Standards, and the Trust Data Protection Policy.

All ICT use must support statutory safeguarding responsibilities and meet Trust expectations for professional conduct.

3. Acceptable & Unacceptable Use

This document will be reviewed on a bi-annual basis. For all questions in relation to this policy, please contact IT on itsupport@graceschools.org.uk

This policy outlines acceptable of IT software, internet, email, social media, via laptops, PCs, tablets, mobile phones and other portable devices. It has a focus on all staff and agents working across the Trust.

The purpose is to ensure safe and acceptable use of technology for the use of communication and delivering education or support for education alongside personal use of the above. It lists the responsibilities that all staff and agents must ensure that any form of communication using technology is used appropriately and in line with GDPR rules.

The Trust/schools aim to ensure that everyone has good access to IT to enhance their role and to be able to provide the relevant learning opportunities for pupils.

All staff and agents must understand that the Trust/schools will monitor the use of ICT systems including email and other digital communications.

Acceptable use includes professional duties only, responsible behaviour, and compliance with Trust procedures.

Unacceptable use includes:

- misuse of data,
- accessing inappropriate content,
- bypassing filters,
- using personal cloud accounts,
- installing unapproved software, or
- sharing confidential information.

Trust staff and agents must ensure that they take responsibility for reading and upholding the standards laid out in this policy.

4. Accounts & Google Workspace

Staff must use Trust Google Workspace for all communication, file storage and collaboration.

Personal accounts such as Gmail, iCloud, Dropbox, or personal Google Drive may not be used to store or transfer Trust information.

Syncing Trust data to personal devices is only permitted within Trust-managed Mobile Device Management containers.

5. Use of Trust Devices

Trust devices are issued for work purposes only and should not be used for personal browsing, email, messaging, social media, shopping, or entertainment.

Devices must be locked, encrypted and kept secure at all times.

No software may be installed without IT approval.

Trust/school equipment is not used to up- or download any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography, etc, covered by the Obscene Publications Act) or anything that is inappropriate or may cause harm or distress to others.

It is not acceptable to use any device for bullying, harassment or discrimination of others, in any form.

There must be no downloading, copying, or distributing anything protected by copyright.

If there are concerns about receiving an unexpected email, staff should contact the person by telephone before opening it, to ensure its credibility. If they are advised it was not sent by that person, they must contact their IT support team and Grace Schools DPO for IT to investigate and keep the DPO updated on the outcome(s).

When replying to personal email addresses the reply does not include attachments that contain personal data. Attachments containing personal data must always be sent via a Trust email addresses, with any attachments encrypted.

6. Personal Devices & "Bring Your Own Devices" (BYOD)

Personal devices may only be used for Multi Factor Authentication ("MFA") or Trust-approved Mobile Device Management ("MDM") applications.

Trust data must not be downloaded, stored, or processed on personal devices outside authorised systems.

Personal devices must not be used to capture images or videos of pupils.

7. Passwords & Multi Factor Authentication

Personal mobile phones are allowed to be used for accessing multi factor / two factor authentication apps when required for work related systems. Personal mobile phones should not be used in classrooms for any other purposes.

All technological devices have password/encryption facilities installed (for mobiles this must be a minimum of a 4-digit passcode).

Passwords must follow NCSC's Three Random Words guidance. (https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words)

Multi-Factor Authentication is mandatory for all systems, with phishing-resistant options preferred.

Passwords must never be shared or written down in insecure locations.

Passwords must not be shared or disclosed to others and staff will not attempt to gain access to other passwords or devices.

Passwords should not be written down and kept where they may be accessed. Passwords are not stored for sites within browsers, e.g. Internet Explorer/Chrome, etc.

8. Communication & Professional Conduct

Professional standards apply to all online communication, including tone, content, and confidentiality.

Staff must use only Trust-approved platforms such as your Grace Schools Gmail account, Google Chat, Google Meet, and MIS systems for work communication.

WhatsApp, SMS, Facebook Messenger and personal email may not be used for Trust business. Your Grace Schools Google Chat account should be used instead.

Staff do not participate in communicating with pupils/parents outside of their role at the Trust when using work or personal technology/devices for the use of social media, texting, calling, etc. It is important to ensure that a professional relationship is always maintained to prevent any misinterpretation of any actions made.

No personal details are exchanged with pupils that would allow contact directly via personal email, telephone or address.

All communications with pupils must be via the Trust's/school's internal network.

If there are concerns about receiving an unexpected email, staff contact the person by telephone before opening it, to ensure its credibility. If they are advised

it was not sent by that person, they must contact their IT support team and Grace Schools DPO for IT to investigate and keep the DPO updated on the outcome(s).

When replying to personal email addresses the reply does not include attachments that contain personal data. Attachments containing personal data must always be sent via a Trust email addresses, with any attachments encrypted.

Staff do not participate in communicating with pupils/parents outside of their role at the Trust when using work or personal technology/devices for the use of social media, texting, calling, etc. It is important to ensure that a professional relationship is always maintained to prevent any misinterpretation of any actions made.

No personal details are exchanged with pupils that would allow contact directly via personal email, telephone or address.

9. Data Protection & Information Handling

Staff must follow Trust data protection policies, ensuring access only to information required for their role.

Sensitive data must be encrypted when transmitted and stored securely.

Any suspected or actual data breach must be reported immediately to the Grace Schools DPO.

10. Filtering, Monitoring & Online Safety

Trust systems are monitored for safeguarding, cyber security, and compliance.
All internet use on Trust devices and networks is subject to filtering and logging.

Staff must not attempt to bypass filtering systems or use VPNs/proxy tools.

11. Artificial Intelligence ("AI") use

Only Trust-approved AI tools may be used for work purposes.

Personal data, pupil information, or confidential content must not be entered into AI systems.

AI output must always be checked for accuracy, bias and appropriateness.

AI cannot replace professional judgement, assessment or safeguarding decisions.

12. Remote Working & Offsite Use

Staff must ensure devices taken offsite remain secure and used appropriately.
Public Wi-Fi should be avoided unless using secure Trust VPN or approved connections.
Printed materials and physical documents must be protected from unauthorised access.

13. Incident Reporting

Staff must report cyber threats, suspicious emails, lost.

Staff must report cyber threats, suspicious emails, lost devises, unauthorized access attempts or safeguarding concerns immediately to IT, the DSL or the Grace Schools DPO.

If any work device is stolen (laptop/mobile phone/iPad or similar), it must be reported to the Trust's Data Protection Officer (DPO) on dpo@demat.org.uk **immediately** as this is considered a breach under GDPR, and the DPO will may need to report to the UK Information Commissioners Office within 72 hours.

Prompt reporting is essential to protect Trust systems and data.

14. Social Media use

The use of Trust/school equipment to access personal sites (social media) is not acceptable.

Any incidents of concern regarding social media misuse are reported immediately to the relevant line manager. This includes but is not limited to illegal, inappropriate or harmful material.

Professional boundaries are maintained when using the internet and social media for personal use. When posting on personal forums/social media staff must ensure that they understand that the use of any comments or photos, regardless of whether they are positive or negative, can be shared with others (parents, pupils, colleagues) and this could lead to losing control of who sees them, or a misinterpretation of what was written: this could then bring your professional role and workplace into disrepute.

15. IT and Information Security

PC/laptop or other equipment remains locked when unattended to ensure unauthorised access is prevented.

Staff respect the technical safeguards which are in place. Any attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services is unacceptable.

All data is kept secure and used appropriately as authorised by the Trust (delegated to the headteacher if school based).

Staff use a Trust or school email address for any correspondence that they send in relation to their role in the Trust/school.

Any emails with attachments that contain personal or sensitive data are encrypted with a password. Password must be sent to the recipient using another transport method or are saved onto a secure shared site, and a secure link is provided that is only accessible by the designated recipient.

Any form of hardware or software should not be inappropriately stored on any Trust-owned device without the Trust's permission or Headteachers permission (delegated to the headteacher, if school-based).

When replying to personal email addresses the reply does not include

attachments that contain personal data. Attachments containing personal data must always be sent via a Trust email addresses, with any attachments encrypted.

There is awareness of where any Trust/school-owned devices are at all times. All devices are stored securely when not in use. Laptops/mobile devices that are taken off-site must be stored securely out of sight. If left in a vehicle they must not be in view but stored securely in the boot with the vehicle locked.

Staff do not use/duplicate/remove or amend anyone else's documents without their prior permission.

16. Enforcement

Breaches of this policy may lead to disciplinary action, removal of system access, safeguarding referrals or police involvement, depending on severity.

All staff are accountable for their actions when using Trust systems and devices.

17. Acknowledgement

There is a commitment by the Trust that ensure that all users of IT in the Trust environment are responsible users, at all times. Any misuse or failure to comply with this policy could result in disciplinary action. The Trust's HR function and the DPO must be notified of any misuse. Any safeguarding concerns will be reported to LADO and in the event of illegal activity the Trust will ensure third party involvement which may include the police.

All staff must read, understand and confirm acceptance of this policy annually via Smartlog in line with Trust requirements.

18. Version Control

No.	*Status of document/changes*	*Prepared by*	*Reviewed by*	*Approved by*	*Date of approval*
Version 4	Staff are required to use multi-factor authentication / two factor authentication for all systems used in Grace Schools, where it is available. Personal mobile phones are allowed to be used for accessing multi factor / two factor authentication apps when required for work related systems. Personal mobile phones should not be used in classrooms for any other purposes.	IT	HR	CEO	June 2025
Version 5	Amended policy issued for the roll out of Google across all Grace Schools	IT	DPO	CEO	August 2026