SHARD Business Services

KEEPING WORK & PERSONAL EMAILS SEPARATE

Key Guidance for Schools & Trusts

SEPARATE • SECURE • PROTECT • COMPLY

Mixing work and personal email creates privacy, security and legal risks. Keep official communication in approved systems so records stay secure, searchable and protected.

This guidance supports GDPR, cyber security and good governance practice for schools and trusts.

WHY SEPARATION MATTERS

- ✓ Protects pupil and staff privacy
- ✓ Reduces phishing and malware risk
- ✓ Prevents accidental data breaches
- ✓ Keeps organisational records secure
- ✓ Supports professional standards

KEY EMAIL SEPARATION PRINCIPLES

1 WHY KEEP THEM SEPARATE?

- ✓ Work emails are not entirely private and may be monitoring lawfully.
- ✓ Mixing personal use reduces your privacy.
- ✓ It reduces risk to your account, network and organisation.

Keep work for work.

2 PRIVACY MATTERS

- ✓ Work emails may be read if there is a valid and legal basis.
- ✓ Personal emails are your private space.
- ✓ Using work email personal things reduces your privacy.

Protect privacy.

3 CYBER SECURITY RISKS

- ✓ Signing up to shopping sites or apps increases your exposure.
- ✓ Data breaches, scams and malware can compromise your work account.
- ✓ A hacked work account can access sensitive school data.

Reduce attack routes.

4 DATA BREACH RISKS

- ✓ You are more likely to send data to the wrong person.
- ✓ Forwarding emails can expose personal or sensitive data.
- ✓ This can cause a data breach and serious consequences.

Think before sending.

5 PERSONAL DEVICES

- ✓ Using personal devices to access work emails increases risk.
- ✓ They may have weaker security and be seen by others.
- ✓ Work data may not be fully protected.

Use approved systems.

6 GDPR RESPONSIBILITIES

- ✓ Personal data must only be processed on approved systems.
- ✓ Transferring data to personal accounts breaches GDPR.
- ✓ ICO enforcement can lean to fines and criminal records.

Be accountable.

SBS INSIGHT HUB

IH-009

KEEPING WORK & PERSONAL EMAILS SEPARATE

Practical continuation page for home working, forwarding, scenarios, checklist and resources.

7 FORWARDING WORK EMAILS

- ✓ Forwarding work emails to personal account is a common risk.
- ✓ Survey data shows 64% of workers admit to doing this to catch up at home.
- ✓ It increases the risk of data breaches an accidental disclosure.

Do not forward work data.

8 WORKING FROM HOME SAFELY

- ✓ Access work emails via an approved systems and devices only.
- ✓ Use secure school/Trust laptops with appropriate security controls.
- ✓ Ensure your home network is secure and up to date.

Keep work at work.

9 LEAVING EMPLOYMENT

- ✓ Do not take any personal data with you when you leave.
- ✓ The ICO has taken action against employees who took data to a new job.
- ✓ This can result in fines and a criminal record.

Protect your future.

10 COMMON MISTAKES

- ✓ Using work email for online shopping, registrations and newsletters.
- ✓ Mixing personal and work conversations.
- ✓ Storing work files or data on personal devices.

Small actions create risk.

11 BEST PRACTICE

- ✓ Use work email only for official business.
- ✓ Keep personal emails and accounts separate.
- ✓ Think before you click, send or forward.

Good habits protect everyone.

12 WHAT TO DO INSTEAD

- ✓ Use the school/Trust system to store and share documents.
- ✓ Use Microsoft 365/Google for collaboration.
- ✓ If you need access form home use approved remote working arrangements.

Use the right tools.

EMAIL SECURITY CHECKLIST

	Yes	No	In Progress	N/A
Work email is used for work purposes only	☐	☐	☐	☐
Staff do not forward work emails to personal accounts	☐	☐	☐	☐
Approved systems are used for documents and collaboration	☐	☐	☐	☐
Personal devices are not used to store work data	☐	☐	☐	☐
MFA is enabled and passwords are strong	☐	☐	☐	☐
Suspicious emails and incidents are reported promptly	☐	☐	☐	☐
Staff do not click links or open attachments when the sender is unknown	☐	☐	☐	☐
Home working arrangements are secure and approved	☐	☐	☐	☐
Leavers do not retain work emails or personal data	☐	☐	☐	☐
Acceptable use and email policies are reviewed regularly	☐	☐	☐	☐

GOOD EMAIL HABITS

1. **Keep Separate** — Keep work and personal emails, accounts and devices separate.
2. **Use Approved Systems** — Access work email and files through approved school systems only.
3. **Think Before Sending** — Check recipients, attachments and links before you click or share.
4. **Protect Devices** — Keep devices updated, secure and protected with strong passwords.
5. **Report Concerns** — Report suspicious emails, incidents or mistakes immediately.

EXAMPLES: WHAT CAN GO WRONG

Shopping site breach

You sign up to a shopping website with your work email. That site is breached and attackers now target your work account.

Malware or scam

A scam email in your personal inbox infects your device. You then access work email and malware spreads.

Accidental disclosure

You forward a work email to your personal accounts and accidentally share it with the wrong person.