**Note For Partner:**

This sales pack can be distributed as is or customised to carry your branding.

To brand this document, simply change the document font, colours and edit the header and footer to carry your logo. Then export as a .pdf file before sharing with clients and prospects.

Alternatively, you can export this document as a .pdf file in its current state and then share with your clients and prospects.



Private email for business

|  |  |
| --- | --- |
| ✓ **Military-grade encryption** | ✓ **To/from any email account** |
| ✓ **Full legal ownership** | ✓ **On any device** |
| ✓ **No tracking, no adverts, no data mining** | ✓ **No downloads or training required** |

StayPrivate enables you to communicate sensitive information with your clients, employees, suppliers and other contacts in a secure, convenient, and compliant way. Designed to fit into your existing email infrastructure with no disruption to your current working practices, and no need for downloads, installations, or employee training.

STAY SECURE

Prevent data leakage and keep information **secure even after** **it leaves** your company email server.

STAY PRIVATE

Keep sensitive corporate information private, including salaries, quotations, transactions, and board minutes.

BUILD TRUST

Show your customers, employees, and other stakeholders that **you care about them** and their data.

STAY COMPLIANT

Ensure your **email communications are compliant** with CCPA, EU GDPR, HIPAA, and other regulations.

STOP PHISHING

Reduce your exposure to phishing and other email-based cyber attacks.

MAKE SAVINGS

Reduce costs, save time & help the environment by using StayPrivate instead of the postal service.

**How does StayPrivate work?**

You simply configure your existing email server to work directly with StayPrivate platform, allowing you to send and receive secure emails directly from your existing email account. This configuration should be handled by your IT administrator.

Once configured, using StayPrivate is easy. Simply include a special keyword1, like #secure or #stayprivate, anywhere in your email and it will be sent securely – that’s it!

1This keyword can be anything you like. You can have multiple keywords. Keywords can be edited at any time, just contact your IT administrator.

**How do other businesses use StayPrivate?**

As business communication has moved online it has created more opportunities for online crimes, such as phishing and identity theft.

Personal email accounts are an easy target for criminals looking to steal information or money.

**Client Communications**

STAY PRIVATE FOR

Password resets are a security weak point.

Email is not secure, but the postal service is slow and costly, meaning delays and frustration for clients.

**Password Resets**

STAY PRIVATE FOR

GDPR requires you to provide SAR information in a concise, intelligible, transparent, and easily accessible form. It recommends that information should be delivered securely via electronic transfer.

**Subject Access Requests (SARs)**

STAY PRIVATE FOR

Emailing company documents home is convenient and sometimes necessary. But it is not secure and often against company policy.

**Working from Home**

STAY PRIVATE FOR

Unprotected email invoices are easily intercepted.

Use StayPrivate to ensure that invoicing and payment information is secure at all times.

**Invoicing**

STAY PRIVATE FOR

Emailing personal information, such as CVs, P45s, illness, complaints and disciplinary information is common practice but not GDPR-compliant.

**Employee Correspondence**

STAY PRIVATE FOR

**Pricing**

StayPrivate is priced based on the number of unique recipients contacted securely over a 12-month period. For most businesses, this number will be close to their total number of clients.

**≤ 100 Recipients: £10 pm**

Includes 10GB of storage

Extra units of 25 recipients: £2.50 pm

Extra units of 10GB storage: £2.50 pm

**≤ 500 Recipients: £40 pm**

Includes 50GB of storage

Extra units of 125 recipients: £10 pm

Extra units of 50GB storage: £10 pm

**Unlimited Recipients: £90 pm**

Includes 100GB of storage

Extra units of 100GB storage: £15 pm

**What do other businesses say about StayPrivate?**

*"StayPrivate is just so easy to use - both for us and our clients. It's secure email, file sharing and storage all in one place."*

David Seager

Development Director, SIFA

*"StayPrivate brings the simplicity and convenience of social media apps to the corporate world, without the security tradeoff."*

Greg Merten

Head of Strategic Alliances,

Blackberry

*"I knew we had a top class internal set up, but once emails left the building that counted for nought. StayPrivate solved our problem instantly and elegantly."*

Steve Cook

Principle & Portfolio Manager, Sequoia

**Frequently Asked Questions:**

Will StayPrivate work with my current systems?

Yes, StayPrivate works with any email account. Your email server needs to be configured to work with StayPrivate - your IT professional should be able to do this for you - and that is it.

My email server is secure. Why do I need StayPrivate?

Enterprise email servers are usually well-protected so that emails between enterprises are normally secure. The problem is the lack of protection for emails which are sent or received outside of the enterprise environment - for example, emails to and from clients, employees, advisers, consultants, non-execs, small companies, and other similar contacts.

StayPrivate ensures that every email your organisation sends remains secure at all times - and the replies too.

How does StayPrivate Keep data secure?

StayPrivate deploys a wide range of security, anti-phishing, privacy, and legal measures to ensure that your information remains safe and secure at all times. These include:

 Military-grade AES256 encryption

 Point-to-point encryption with dynamically generated keys

 Strict email verification, volume limits and active blocklisting

 All communications organised into private channels

 Enforced multi-factor authentication using StayPrivate's patented click-and-PIN technology

 Triple geographic redundancy and resilient architecture

 Robust legal framework

 Expert support

Who can receive private emails?

Anyone!

StayPrivate handles emails differently depending on whether the recipient email address is corporate or personal. Emails to/from free email providers (such as Gmail, Outlook, Yahoo) are stored in the StayPrivate secure environment.

For corporate email accounts, we use TLS encryption to ensure the security of the email whilst in transit. Once the email arrives at the corporate server, the organisation takes over the duty of care - just as it does when it takes delivery of a physical item through the post.

If the corporate email server does not support TLS encryption, we ensure the email remains private by sending it the same way as we do for personal emails.

How does StayPrivate differ from traditional email encryption solutions?

Just as you would expect any enterprise-grade email encryption solution, StayPrivate offers excellent security, durability, and control. What makes StayPrivate different is that it is so simple, easy, and enjoyable to use. Both for the company and for its contacts.

StayPrivate is integrated at an email server level, meaning that you can be protecting your entire organisation within literally a matter of minutes. There is no need to download any software, perform any ongoing administration, or provide any training to your employees, saving you time and money.

StayPrivate leads the market with its customer experience. The combination of clean, modern user interfaces mobile apps, company branding, and patented 'no trail PIN' technology, mean that StayPrivate is a pleasure to use for your customers and other contacts.