Privacy Policy Including Personal Phone Use

EXCELLERATE SERVICES

WHERE BETTER BEGINS

Introduction to Excellerate Services UK

Our organisation is made up of brilliant people. Each of us is unique, whether in terms of our background, personal characteristics, experience, skills or motivations. And we value our people for the differences they bring to the table. These differences - this diversity - is powerful. Fostering an inclusive culture helps each of us to benefit from a wider range of these different perspectives, experiences and skills. We believe that this creates a happier, more productive working environment for us all.

1. Purpose & Scope

Excellerate Services UK Ltd is committed to ensuring all colleagues are paid accurately for the hours they work. This policy sets out the mandatory requirements for recording working time using the Company's approved systems.

The purpose of this Privacy Policy is to explain how we collect, use, store, share, and protect personal information when individuals interact with our services, systems, and communications. This includes outlining our approach to data protection in relation to personal phone use, whether employees use personal devices for work-related activities or connect them to company networks.

The policy ensures transparency, supports compliance with applicable data protection laws, and helps individuals understand their rights and responsibilities when their personal data is processed by us.

Scope

This policy applies to:

- All employees, contractors, agency workers, and third parties who interact with our systems or provide personal information to us
- All personal data processed by Excellerate Services UK Limited, whether collected online, in person, or through digital systems
- All devices used to access company systems, including:
    - Company-issued mobile phones
    - Personal phones used for work-related purposes (e.g., email, Velocity, MFA authentication)
    - Personal phones connected to company Wi-Fi or networks

The scope includes, but is not limited to:

- Data collected through our website, applications, and communication channels
- Data processed for authentication, security, and system access
- Logs and metadata generated when personal devices interact with company systems
- Any processing required to maintain security, investigate misuse, or comply with legal obligations

This policy does **not** apply to personal content stored on an individual's own device (e.g., photos, messages, personal apps), which remains private and is not accessed or monitored by us.

2. Policy Governance

- Policy Owner:
  - Chief Financial Officer
  - Head of Compliance & Risk
- Oversight Body:
  - Reviewed by Chief Financial Officer
- Signed off by CEO
- Review Schedule:
  - Annual review
  - Review log (with version control and sign-off by oversight body)

3. Commitment to Frameworks

- Alignment with:
  - Working Time legislation

4. Responsibility Matrix (RACI)

Activity / Responsibility	Policy Owner	Data Protection Officer	IT / Security Team	HR	Managers / Supervisors	Employees / Users
Drafting and updating the Privacy Policy	A/R	C	C	C	I	I
Approving the Privacy Policy	I	Exec Team (A)	I	I	I	I
Ensuring compliance with data protection laws	C	A/R	C	C	I	I
Managing personal data requests (access, deletion, etc.)	C	A/R	I	I	I	I

Activity / Responsibility	Policy Owner	Data Protection Officer	IT / Security Team	HR	Managers / Supervisors	Employees / Users
Implementing technical controls for device and data security	I	C	A/R	I	I	I
Managing Mobile Device Management (MDM) or BYOD controls	I	C	A/R	I	I	R (if using personal phone)
Monitoring network and system access logs	I	C	A/R	I	I	I
Investigating data breaches or misuse	C	A/R	A/R	C	C	I
Delivering training and awareness	C	C	I	A/R	R	R (participation)
Enforcing compliance with acceptable use and personal phone rules	I	C	C	C	A/R	R
Reporting incidents or suspected breaches	I	I	I	I	R	A/R
Maintaining records of processing activities	C	A/R	C	C	I	I
Managing employee data and HR-related privacy matters	I	C	I	A/R	C	I
Ensuring personal devices meet minimum security standards	I	C	C	I	R	A/R
Communicating policy changes	R	C	I	A/R	R	I

Key

- R – Responsible: Performs the task
- A – Accountable: Ultimately answerable; approves decisions
- C – Consulted: Provides input or expertise
- I – Informed: Kept updated but not directly involved

5. Communication & Accessibility

- Published on:
  - External website
  - Internal intranet
  - Electronic Noticeboards
- Included in:
  - Annual compliance and refresher training
  - Management Review

1. Introduction

This Privacy Policy explains how we collect, use, store, and protect personal information when you interact with our services, systems, and communications. It also sets out how personal data is handled in relation to personal phone use, whether on company premises, using company networks, or when accessing work systems from a personal device.

We are committed to protecting your privacy and ensuring compliance with applicable data protection laws, including the UK GDPR and Data Protection Act 2018.

2. Who We Are

Excellerate Services UK Limited is the data controller responsible for determining how your personal information is processed.

3. Information We Collect

We may collect the following categories of personal data:

a. Information you provide directly

- Name, contact details, and employment information
- Communications, enquiries, or feedback
- Information submitted through forms, systems, or applications

b. Information collected automatically

- Device identifiers (e.g., IP address, device type, operating system)
- Network activity (e.g., connection logs, access attempts)
- Usage data when accessing company systems or networks
- Cookies and tracking technologies on our website

c. Information related to personal phone use

We do **not** access the personal content of your device (e.g., photos, messages, call logs). However, when a personal phone is used in connection with our services or networks, we may collect:

- Phone number (if used for authentication or communication)
- Device information (model, OS version, security status)
- Network connection logs when connected to company Wi-Fi
- Activity logs when accessing company systems, apps, or email
- Location data **only** if required for specific security features (i.e., clocking in and out)

d. Information from third parties

- Service providers
- Security or authentication tools
- Publicly available sources

e. How We Use Your Information

We process personal data for the following purposes:

- Providing and improving our services
- Managing user accounts and authentication
- Ensuring system and network security
- Monitoring compliance with company policies
- Supporting investigations into security incidents or misuse
- Communicating important updates or alerts
- Meeting legal, regulatory, or contractual obligations

4. Personal phone use

Where personal devices are used for work-related purposes (e.g., email, Velocity, MFA authentication), we may process data to:

- Verify identity and secure access
- Protect company information and systems
- Monitor for unauthorised access or security risks
- Support remote-wipe or access-revocation functions (company-issued devices only)

We do **not** monitor personal activity unrelated to work.

5. Legal Basis for Processing

We process personal data under one or more of the following lawful bases:

- **Consent** (e.g., opting into MFA using a personal phone)
- **Performance of a contract**
- **Compliance with legal obligations**
- **Legitimate interests**, such as ensuring security and preventing misuse

6. How We Share Your Information

We may share personal data with:

- Trusted service providers (e.g., IT, security, cloud services)
- Professional advisers
- Regulatory authorities where legally required
- Third parties involved in incident response or investigations

Clients and their authorised screening providers, where required, to obtain security clearance, complete background screening (including Baseline Personnel Security Standard (BPSS) checks) or meet contractual site access and security requirements. In such cases, we will share only the minimum personal data necessary to facilitate the screening process and will ensure appropriate safeguards are in place.

We do **not** sell personal information.

7. International Transfers

If personal data is transferred outside the UK or EEA, we ensure appropriate safeguards are in place, such as Standard Contractual Clauses.

8. Data Retention

We retain personal data only for as long as necessary to fulfil the purposes outlined in this policy or to meet legal and regulatory requirements.

Data relating to personal phone use (e.g., access logs) is retained only for the minimum period required for security and audit purposes.

9. Your Rights

You may have the right to:

- Access your personal data
- Request correction or deletion
- Object to or restrict processing
- Withdraw consent
- Request data portability

To exercise these rights, contact us using the details below.

10. Cookies and Tracking Technologies

Our website uses cookies to support functionality, analytics, and performance. You can manage cookie preferences through your browser settings.

11. Security

We implement appropriate technical and organisational measures to protect personal data, including encryption, access controls, and monitoring for suspicious activity.

For personal phone use, we may require minimum security standards such as:

- Device passcode or biometric lock
- Up-to-date operating system
- Prohibition of jailbroken or rooted devices

12. Personal Phone Use Expectations

To protect both personal and company data:

- Personal devices must not store sensitive company information unless authorised.
- Work-related apps may enforce security controls (e.g., MFA, remote wipe of work data only).
- Company Wi-Fi usage may be logged for security and compliance.
- Personal content on your device remains private and is not accessed by us.

13. Links to Third-Party Sites

Our website or systems may link to external sites. We are not responsible for their privacy practices.

14. Contact Us

If you have questions about this Privacy Policy or wish to exercise your rights, please contact:

Justin Moore - justin.moore@excellerateservices.com - CFO

This policy will be reviewed annually or in response to significant changes in legislation, operations, or stakeholder feedback. Updates will be communicated to all staff and partners, and improvements will be tracked through performance indicators and audits.

Signed on behalf of Excellerate Services UK Ltd

Johan Venter, Group CEO UK & Ireland

Issue Date: 28th March 2026