FamilyCare

Healing pasts • Building futures

Mobile Phones Policy

www.family-care.co.uk

Mobile Phones Policy

Implemented/Reviewed: July 2025

Date of Next Review: July 2026

Policy

Employees within the Family Care Group may be be eligible for a company issued mobile phone if the company deems it is necessary for the performance of that employee's role, or in the Residential Homes there will be a unit mobile available as a shared resource for staff when working off site with young people.

Upon termination of employment, all company-issued mobile devices must be returned to Business Support, and access to company data will be remotely revoked

Procedure

Use of Mobile Phones

Company issued mobile phones are to be used for:

i. Making/receiving calls in connection with the business
ii. Using productivity apps
iii. Business messaging and emails
iv. Internet tethering for business purposes.

All international calls are blocked and picture messages must not be used.

From time to time a personal call may need to be made from a company mobile phone. The Company reserves the right to audit phone usage and unreasonable or irresponsible personal usage may result in reimbursement of associated costs.

Safe Use of Mobile Phones

Use of mobile phones is strictly prohibited whilst driving except where the use of a hands free car kit is available.

Lost, Stolen or Damaged Phones

Company issued mobiles must be properly cared for by the employee who is issued with the phone. This includes not leaving the mobile phone unattended in a vehicle or out of the workplace. If a company mobile phone is lost or stolen you should inform your manager and Business Support immediately so that the SIM card can be suspended. An employee may be held responsible for the cost of the mobile phone if the appropriate care has not been taken.

Damage is to be immediately reported to your manager. An employee may be held responsible for any costs in repairing or replacing a company mobile phone if the damage resulted from the employee's careless actions.

Security

In order to protect the data we hold on the mobile phones and comply with GDPR legislation employees are advised never to connect to public/shared wifi hotspots or foster carers home wifi. There is an adequate data bundle available for business use and this can be increased if necessary by contacting Business Support. Any failure to follow this policy which results in a data breach may result in disciplinary action being taken against the employee.

Personal Mobiles

Use of personal mobiles should be kept to a minimum during working hours. Employees should not access company software via personal mobiles, unless a security measure is in place to access the device (e.g. pin code). If your device is lost or stolen, please inform Business Support as a matter of urgency to allow password resets.