Mobile Phone Policy and Procedures

Last updated: January 2026

Purpose and Scope

This document sets out Kids policy to regulate the issue and use of:

- Kids mobile phones
- Kids mobile phone contracts
- Colleagues' Personal mobile phones
- Third Party mobile phones

This document also sets out Kids position on Service Users use of mobile phones during Kids service delivery.

This policy and guidance applies to all colleagues working on behalf of Kids.

Definitions

Colleagues: The term includes employees, sessional workers, volunteers, students and Trustees of Kids. This is also extended to independent contractors who are undertaking direct work with children or young people on behalf of the charity.

Kids issued mobile devices

Use of Kids issued mobile phones

Kids mobile phones are to be used for making work related calls, texts, taking images of equipment and for expense (i.e. receipts), accessing Kids systems, services and approved applications (i.e. scanning QR codes).

Kids mobile data services should only be used to access the internet for business purposes.

Kids mobile phones **must not** be used to take photographs or videos of children/young people unless the exception process has been followed- Please see Appendix 2. Where images of children/young people are required i.e. for learning and development, to share with parents/carers or for publicity, a Kids issued camera must be used. To protect the privacy of individuals and uphold Kids' safeguarding and data protection standards, photography using mobile devices is strictly controlled.

For further detail re consent, taking, storing and sharing images see Kids Consent for Photography and Videography Policy.

For detail of how to upload images from Kids issued cameras see Appendix 1.

Monitoring Usage
Mobile data is shared across the organisation. ICT monitors monthly usage to make sure the overall allowance is not exceeded. If someone's usage suddenly increases, ICT may ask about how the data was used on their work phone.

Tethering
Tethering is allowed on Kids mobile phones, however, should only be used when traveling or working in locations where no Wi-Fi or Ethernet connection is available and up to a maximum of two hours. Any time needed above this must be agreed in advance by the IT team. Remote & Hybrid colleagues must never use tethering as their primary source of internet.

Blocked services
International calls and premium rate numbers are barred on all devices unless a business need is identified and approved by the Executive team. It is not permitted to use Kids mobile phones to call or message these numbers without this approval. International roaming (outside of the EU member states) is disabled and not permitted. Multi-Media (MMS) messages are disabled and not permitted.

SIM swapping
Kids do not permit the transfer of a Kids SIM card from the supplied handset to a personal device (unless this is done with written consent by the appropriate leader in collaboration with the ICT Department). SIM swapping may incur substantial costs for incorrect tariff usage and Kids will seek full recompense for any additional charges incurred due to this action. Kids would also point out that this may cause serious security breaches where 'data' based devices carry Kids information.

Mobile phone Handsets (Allocation and Care of Handsets)
Kids handsets can be acquired by completing the ICT request/removal form. The local budget holder must approve the monthly tariff cost & the handset cost before the ICT department can assign a colleague/service a Handset.

If a handset needs reallocating to another colleague, the ICT department must be notified as records need to be kept up to date & the device needs to be reset & enrolled in the new colleague's name.

Kids offer a standardised range of handsets, and handset allocation is determined based on business case and cost effectiveness not personal choice.

The user should take all reasonable steps to prevent damage or loss to their mobile phone. This includes not leaving it on view in unattended vehicles and storing it securely when not in use. The user may be responsible for any loss or damage if reasonable precautions are not taken.

If a colleague loses more than two mobiles within any one year period, Kids reserves the right to refuse to issue any further devices to that individual.

Mobile phones remain the property of Kids at all times and must be surrendered when a colleague leaves employment or on demand by leaders or the ICT Department.

Mobile Phone Settings

Mobile Device Management (MDM)
All Kids mobile phones are to be enrolled into the Kids MDM platform (Microsoft Endpoint Manager), this allows ICT to push security, configure & approved applications to devices. If a new application is required a DPIA form is required for ICT to put the application in the store.

PINS & Encryption
All Kids mobile phones are encrypted and require a pin code of 6-digits minimum to unlock the device. This is in place to protect Kids user account information and any sensitive data (e.g., personal data, passwords, or any other data that could bring Kids into disrepute should it fall into the wrong hands). This pin, or other security lock should be treated like any other password and should never be shared, and the device is to be used by the person it is allocated too only. If for any reason it is suspected that security measures are not working the ICT Department must be informed immediately.

Support
Kids ICT department is responsible for providing support for Kids owned mobile phones and ensuring access to services and applications. Each user is responsible for ensuring the mobile phone is used primarily for company business.

Contracts obligations
Having placed an order for a mobile phone, users are entering into a two-year contract with the service provider. The user is therefore issued with the device for a minimum period of two years. The device is available to the user if they remain with Kids and their role requires them to be available for contact outside of the office.

Managing mobile phone contracts
The local budget holder is responsible for:

- reviewing the ongoing requirement / eligibility for each mobile device funded from their budget;

If a user changes project code, you must inform the ICT department. This will allow costs to be allocated appropriately.

Governance requirements
Managers with authority to approve mobile phone requests have ultimate responsibility and accountability for ensuring that Kids Mobile Phone Policy and Procedures are applied to all mobile phones within their departments. Managers who have authority to approve mobile phone requests must apply the Mobile Phone Policy and Procedures to all requests within their defined authority and must not act outside of that authority.

Colleagues Personal Mobiles

With the exception of Community Short Break Sessional Colleagues (see below), colleagues should not have personal mobile phones on their person when working directly with children and young people. Colleagues should leave personal mobile devices inside their bags/stored in lockers/offices during contact time with children/people.

Colleagues must only use personal mobile phone numbers for work purposes to get codes/calls for multi factor authentication to access services and/or to access Kids related applications.

On personal mobile phones colleagues must only access applications which support Microsoft App Protection Polices, this ensures all Kids data is kept secure on the device. If access is required to web based applications such as Direct Short Breaks or Focalpoint these should be accessed through the Microsoft Edge app, not Safari, Google Chrome etc.

When using a personal mobile, colleagues are using personal data at their own risk & Kids will not reimburse colleagues. When on a Kids site colleagues have the option of connecting to the Kids – Guest network so they are not required to use own mobile data.

Using a personal mobile number to contact internal or external stakeholders is not permitted unless prior approval is given by an Executive member and would be classed as a data breach.

Community Short Break Sessional Workers – Personal Mobiles

Community Short Break Sessional colleagues are not allocated a Kids Mobile phone. For these colleagues there are conditions under which they may use their personal mobile phones during work hours, ensuring that such use aligns with Kids commitment to safeguarding children and maintaining professional boundaries.

Community Short Break Sessional colleagues are permitted to use personal mobile phones:
- When necessary for work-related calls, messages or access to Kids related applications provided that such communication is documented and conducted transparently.
- for emergency situations or essential work-related communication when no alternative is available.

Under no circumstances must Community Short Break Sessional Workers use Personal Mobile phones to take any photographs or videos of children or young people.

Third Party (i.e. Parents/Carers) mobile phones/other devices

Third parties must not use mobile phones or any other devices to take photos of children and young people, including those they are responsible for whilst on Kids premises or at Kids organised events and all third parties must be advised of this during the signing in process.

Service User Mobile Phones (Children and Young People whilst in receipt of Kids services)

Kids understands that the use of mobile phones is popular among children and young people. However, to safeguard everyone in receipt of Kids services colleagues are to discourage children/young people's use of mobile phones during service delivery.

If a child/young person must use a mobile phone during service delivery for a specific need this must be part of the child/young person's risk assessment. Children/young people must not be allowed to use personal mobile phones to take images of children/young people or colleagues during service delivery.

Any concerns in relation to children/young people use of personal mobile phones during Kids services must be reported in line with Kids Safeguarding Children and Adults Policy and Procedures.

Training on this policy and procedure will be given during induction and updated through line manager briefings.

Failure to comply with this policy may lead to disciplinary action which could include summary dismissal or as grounds to terminate your contract with Kids. Where relevant, any excessive data or other usage costs will be recouped.

References and Associated Documents

All colleagues applying for or using a mobile phone for business use must comply with the requirements of all relevant and applicable legislation and associated documents:

- Data Protection Act 2018
- Freedom of Information Act 2000
- Kids Personal Conduct Policy
- Kids Photography and Filming Policy
- Kids Professional Boundaries Policy
- Kids Safeguarding Children and Adults Policy and Procedures

- Kids Social Media Policy and Procedures
- Kids Use of IT Policy and Procedures
- Regulation of Investigator Powers Act 2000
- UK – General Data Protection Regulations

Appendices

Appendix 1 – Camera Guide
Appendix 2 – Use of mobile devices for photography

Transferring Photos to a Computer

1. Connect the camera to the computer using the supplied USB cable:

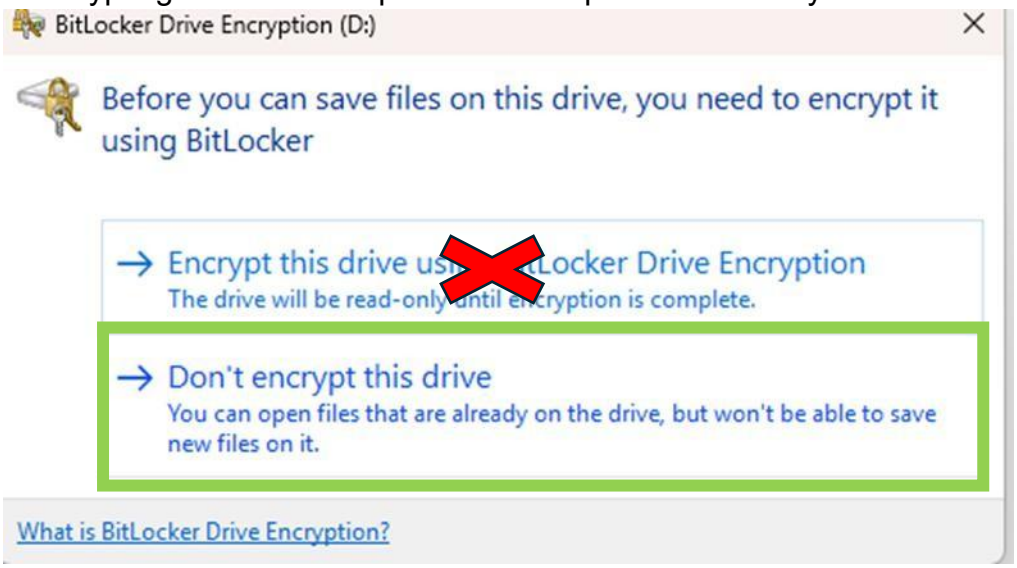
- Plug the USB-A end into the computer.

- Plug the USB-C end into the camera.

2. When prompted with a BitLocker Drive Encryption message, **DO NOT** select "Encrypt this drive."

- Instead, click Don't encrypt this drive.

- Encrypting will erase the photos and require the memory card to be reformatted.



3. Open File Explorer (yellow folder icon on the taskbar).

4. In the left-hand panel, locate and click on the USB Drive (the drive letter may vary).

5. Inside, you will see two folders: PHOTO and VIDEO.

6. To transfer photos:

- Open the PHOTO folder.

- Right-click on the images you want to copy.

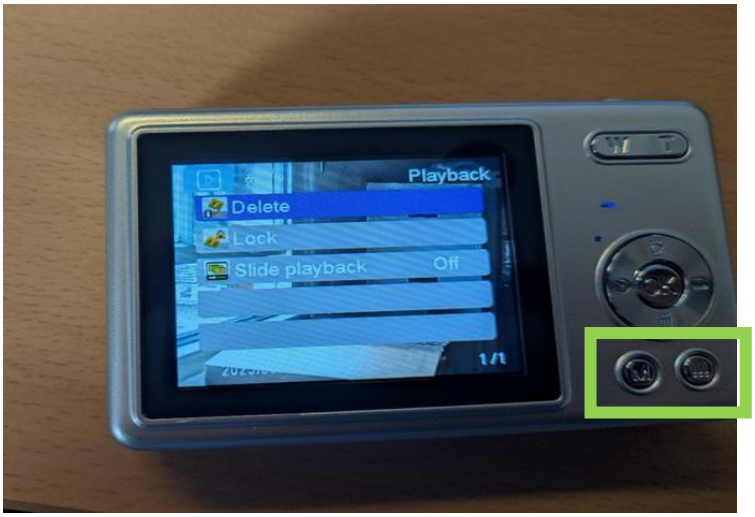
- Select Copy, then Paste them into a folder on your computer.

Deleting Photos

Photos can only be deleted directly on the camera. There is no option to delete photos from a computer.

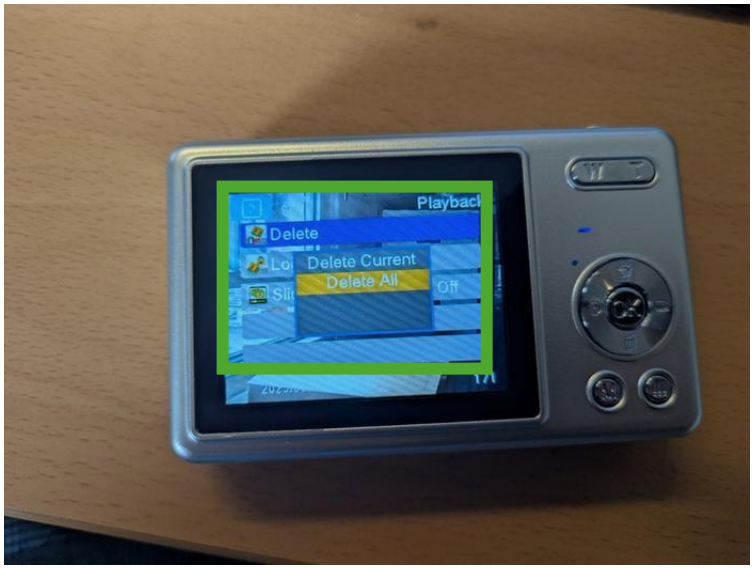
1. Press the M button (bottom right) until you reach the gallery of photos you've taken.

2. Press the button with the three lines (≡) on it.



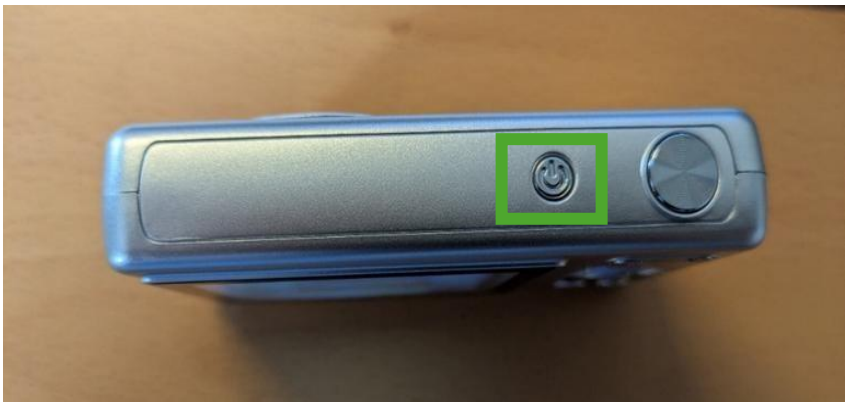
To Delete All Photos:

3. Select Delete > Delete All.

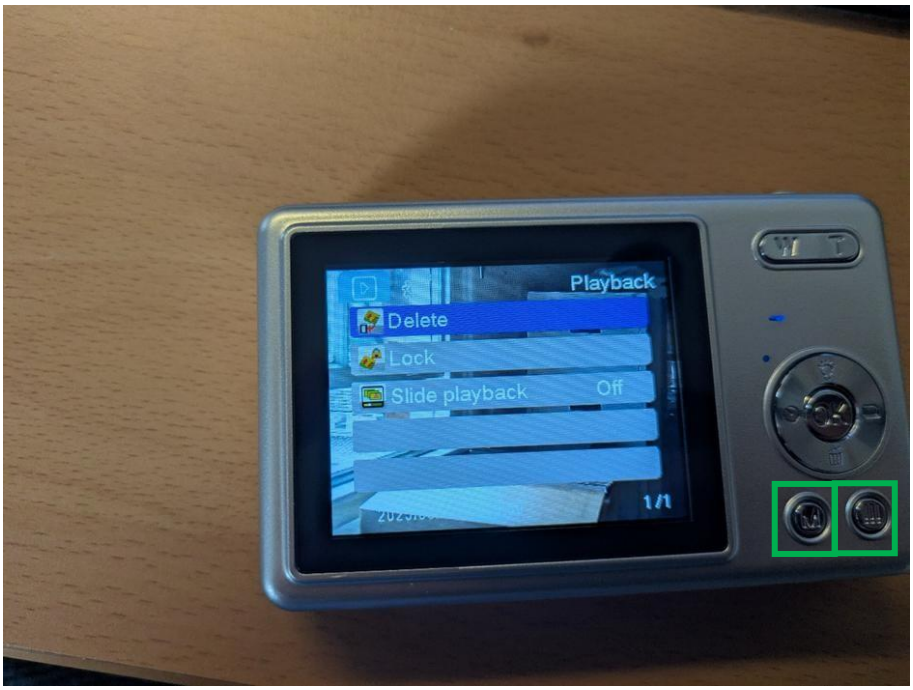


To Delete a Single Photo:

1. Press the Power button on top of the camera to go back.



2. Press the M button again until you return to the photos.
3. Use the navigation buttons to scroll to the photo you want to delete.
4. Press the ≡ (three lines) button.
5. Select Delete > Delete Current.



Appendix 2 - Use of Mobile Devices for Photography

Purpose

This appendix outlines the conditions under which photographs may be taken using a company-issued mobile phone or a third-party mobile device during Kids' activities in exceptional circumstances.

To protect the privacy of individuals and uphold Kids' safeguarding and data protection standards, photography using mobile devices is strictly controlled.

Conditions for Approval

1. **Executive Team Authorisation**
    - Photographs may only be taken with prior written approval by a member of the Executive team and this must be recorded in the ELT Decision Log.
    - Approval must specify:
        - **Purpose** of the photography (e.g., event documentation, marketing content).
        - **Duration** for which photography is permitted.
        - **Designated individuals** authorised to take photographs.
2. **Permitted Devices**
    - Company-issued mobile phones may be used by authorised colleagues.
    - Third-party mobile devices may only be used by individuals explicitly approved by a member of the Executive Team.
3. **Scope of Use**
    - Photographs must only be taken for the approved purpose and within the approved timeframe.
    - Images must be handled in accordance with Kids **Data Protection Policy** and **Safeguarding Guidelines**.
4. **Storage and Transfer**
    - All photographs taken on company devices must be transferred to secure charity systems within 24 hours.
    - It must be agreed with any third party where the images will be stored i.e. on personal or third-party device and for what timeframe.
5. **Prohibited Actions**
    - Unauthorized photography is strictly prohibited.
    - Sharing images on personal social media accounts or with external parties without explicit consent is not allowed.

Compliance

Failure to comply with this appendix may result in disciplinary action and/or withdrawal of mobile device privileges.