WORKING REMOTELY DATA PROTECTION GUIDANCE FOR CHILDREN'S SERVICES

Supporting Guidance

We **all** have a **legal duty** under UK General Data Protection Regulation (UK-GDPR) to keep the personal information we hold safe and secure.

We **all** have a **responsibility** to service users, staff, donors, volunteers, and others to keep their information safe, only allow the appropriate people to have access to it, and to only hold the information for the appropriate length of time.

To assist you to adhere to these responsibilities whilst working either from home or remotely, the following document has been developed in 3 parts to guide you through your data protection considerations.

- **SECTION 1**: Is a Data Protection Checklist for Managers. It should provide all managers with list of considerations & responsibilities that need to be monitored with teams to ensure data protection is complied with whilst working remotely.
- **SECTION 2**: Provides an overview of the key guides and policies that will support you to work safely and securely whilst working remotely.
- **SECTION 3**: Provides more in-depth guidance on some of the key guides and policies.

MANAGER'S CHECKLIST

SECTION 1: Working Remotely – Data Protection Checklist for Managers

Requirement	Met/Not Met/N/A	Action
Alert staff that they should not download confidential/sensitive information onto Personal Devices.		
Ensure staff are aware of their responsibilities around storing and shredding of printed documents		
Enable staff to securely keep any temporary work in progress 'hard copy' records at home and to appropriately shred them when no longer required.		
Advise staff of the requirement not to store personal data on their devices. Information should be stored in the Service's Recording System in line with Recording and Safeguarding policies.		
Advise staff that where they are using personal phones, appropriate safeguards should be in place (e.g. do not use non-Barnardo's email addresses, Screen calls …).		
Remind staff of the requirements to keep personal and sensitive information secure. In practice, be mindful when making calls around non-Barnardo's employees, unattended screens should be locked, and hard copy documents should not be left out.		
Advise staff to use 'Teams' for remote video meetings and where not possible/appropriate, advise staff on security measures for alternative Applications.		
Advise staff that all video and photo material need to be appropriately consented and recorded.		
Alert staff to remote 'Consent to receive service' & YDYR processes, so that DP does not become a barrier.		
Ensure that physical post to the office is either re-directed or collected regularly. Be particularly aware of Subject Access Requests (SARs) & court requests.		
Inform staff of their requirements in sending emails securely and appropriate use of BCC.		
Ensure staff are up to date with Data Protection Training.		
Alert staff to the Breach process and remind them of their responsibilities.		

Undertake regular housekeeping to ensure information continues to be deleted, archived, or destroyed in line with Barnardo's retention policy.		
Advise staff to consider whether they actually need to use personal data to complete a task. If they do, use the minimum amount possible.		

GUIDANCE

SECTION 2: Working Remotely – Data Protection Guidance

Overview:

Working with Barnardo's Equipment

Guidance on accessing B's systems from home

Working with non-Barnardo's Equipment/Systems

The above factsheet provides advice. The key reminder to staff is '*ensure you protect all our data. Do not download any sensitive files to your personal device'.*

- **Computers/devices:**
  - You will need an OKTA Login, to access B's systems on your personal equipment. Sign up to Okta on the Passwords and signing in page, then Go to login.barnardos.org.uk. If you can access Inside Barnardo's, the Accessing Systems from Home page will be helpful.
- **Phones:**
  - Download Microsoft Outlook to manage emails and calendar remotely.
  - Ensure that staff and volunteers using personal phones operate number screening to obscure their number. Do not share personal numbers with service users and do not store personal data on personal phones (includes SU phone numbers and texts for example).

Advice in relation to applications

In the context of remote working, we have all transitioned to the use of video conferencing applications. Each have their different merits. With an Organisational shift to Microsoft 365 and the role out of new IT Equipment, the advice is to use 'Teams' wherever possible. We have clarity on the security of this platform, and it will be supported by the Helpdesk.

- **Teams** – This is Barnardo's preferred option. This should be used where possible for all meetings we organise. Further guidance below.
- **GMeets** – Google is no longer a Barnardo's product so GMeet should not be used for Barnardo's virtual meetings. You can continue to participate in GMeet if you are invited by an external organisation.
- **Zoom** – We have security concerns in relation to this platform, see further guidance below.
- **WhatsApp** may be used to communicate with service users as long as they are 16 or over the following is an example of Guidance on use of WhatsApp is followed.
- **Security considerations:**

- Recording of sessions – technically we cannot stop service users from recording sessions. See guidance below as to how best to protect all parties.
- Recording of Photos or Videos. See 'Contributions and Informed consent' guidance.

Maintaining Security

- Obtaining Consent virtually – Data Protection should not be a barrier, having a physical signature to work with C&YP as an example, is not a necessity, if you follow the guidelines below.
- Subject Access Requests (SARs) – Ensure that SARs continue to be acknowledged and processed in a timely manner. See further guidance below.
- Paper Records outside of the office – Consider the security of any paper records being processed outside of a Barnardo's secure space. Records containing personal information should be kept in a lockable storage space when not in use (box/draw etc). Your service must consider how paper records will continue to be shredded appropriately.
- Work related calls in private – Consider the sensitivity of information being discussed and where possible try to undertake sensitive calls in a private space.
- Technology outside of the office – Consider any devices that can "listen in" when working at home or on non-Barnardo's premises, such as Alexa. These should be removed or disabled.
- Secure Emails – Information about how to encrypt using Microsoft 365 is available here.
- Data Breaches – The process for managing data breaches can be found here and the form that needs completing is here. Critically, this process should be completed as soon as a breach is detected (even if just suspected), you should not wait for a manager before submitting to dataprotection@barnardos.org.uk.

Data Protection Training

All staff should complete the Barnardo's Mandatory Data Protection training available through BLearning. The Mandatory course that must be completed is Data Protection and Security training.

Other related Barnardo's guidance and policies:

- Information Security Policy
- Data Protection Policy
- IT Code of Conduct
- Data Protection: Jargon Buster
- Recording Policy
- Safeguarding Policy

SECTION 3: Further detailed guidance

Guidance around use of Teams

This is the preferred platform to be used.

Additionally, there are some useful training tips from Microsoft available here.

Guidance around use of Zoom

The overriding guidance is, that as we transition across to our new 'Kit' and Microsoft 365, we should be using 'Teams' as our primary video conferencing application. If it is essential to use 'Zoom', then these considerations should be made in order to mitigate the risks to data security:

1. Firstly – can you use a licensed version?
2. Ensure Zoom is kept updated - Zoom US advises users to make sure users have the latest version of the software. It is recommended that when joining a Zoom meeting you should "join from browser" (there is a tick box for this as you launch a meeting)
3. The host should set new login details and a new password for each meeting
4. Do not use Zoom for sharing sensitive/confidential information
5. If you plan to record sessions a DPIA should be undertaken to demonstrate how risks are mitigated

Obtaining Consents and Agreements when you are not having direct contact with service users or carers.

Being unable to obtain a service user or parent's signature during the pandemic does not prevent you working with them. If you cannot send it to them by email; explain the content of the document and obtain their verbal agreement, consent or acknowledgement and record this. If you use e mail to share a form that needs a signature a response via e mail can be used to confirm the consent or agreement and this may be saved to the case file. Please ensure that there is nothing in the email trail that should not be saved. Obtain the signature or provide the document when you are again able to have contact. Here are some specific examples:

- **Your Data Your Rights.** If you cannot e mail a copy of this; explain what you will be recording and why, if you routinely share their data with another organisation explain with whom and why, say how long the data will be kept for and how it may be accessed. Record the content of your discussion in the case file or other record as appropriate.
- **Parental agreement to receive a service.** If this cannot be obtained via e mail; obtain verbal agreements and record this. Obtain signature when direct contact is resumed.
- **Consent.** If consent is required is required in order to share information with a third party and cannot be obtained via an email; obtain verbal consent and record this as soon as possible. Obtain the signature when you are able to.
- **Complaints.** If possible, use e mail to share the CR 1 and 2 (see Complaints Policy for further info) and use e mail confirmation to evidence that the complainant is happy with the content. If this is not possible explain the content and obtain and record verbal consent.

Subject Access Requests (SARs)

- This procedure provides instructions on dealing with Subject Access Requests (SARs). You may wish to use Barnardo's SAR Form, although this format is not a requirement and we should not insist that it be used. The following flow chart for managing SARS may be useful – See Inside Barnardo's
- The current situation may impact on the speed with which we can respond to SARs or receive responses from 3rd parties about sharing their data. Please use this Letter informing subjects of possible delays to SARs if the impact of the current situation on your service operations, is likely to impact the speed of response.
- Services operating remotely should have a mechanism to check for any paper requests that may continue to be sent to the office base.
- It is likely that if a service receives a SAR, that some form of redaction will need to take place. In order to undertake redactions electronically, specialist software is required. If the Service does not already have access to Adobe Pro, please contact your MIO in the first instance.

Guidance on the recording of sessions

Technically we cannot stop service users from recording sessions. Where we have an indication that this may be happening, we should acknowledge it and set some clear ground rules. If you are in a session you believe is being recorded and believe this could present a risk, stop the session at an appropriate moment and seek guidance from your line manager. We could be considered a third party, in which case, they would need our consent to share further and in doing so they would obviously need to consider the risks to any children involved. On this basis the Service User must demonstrate the purpose for the recording and then we should establish a written agreement with clear boundaries around limiting the purpose for the recording, agreeing the scope within which it will be shared/used, which we hope would negate the use for any possible other purposes. If agreeable to all, it may be sensible for Barnardo's to undertake the recording of the sessions and share with the service user.

Section 4: Document History

Version	Date	Author	Status	Comment
0.1	March 2021	Sian Patterson/Rob Cope	Draft	This document needs to be reviewed by MIOs and DPO
0.2	April 2021	Sian Patterson/Rob Cope	Draft	Reviewed by MIOs and revised
0.3	May 2021	Sian Patterson	Draft	Reviewed by Martine King and revised
0.4	June 2021	Sian Patterson	Draft	Reviewed by Audrey Barr and revised
0.5	October 2021	Sian Patterson	Draft	Reviewed by Martine King and revised
V1.0	October 2021	Sian Patterson	Ready to circulate	Approved