Civil/crime news: updated guidance on removable media available

New guidance available on GOV.UK explains the legal requirement to only send encrypted removable media in support of applications and bills.

Why are you telling us this now?

We want to remind you about:

How does this affect provider work?

Providers should avoid submitting removable media in an unencrypted state. If we receive unencrypted items, we will still process the information contained on the removable media.

But we are not able to take the risk of data loss by returning unencrypted media either through the post or by DX.

We would like providers to take the same approach and avoid sending unencrypted media in the first place.

What happens to unencrypted items?

If you send unencrypted removable media to the LAA it is your responsibility to arrange for it to be returned securely. If arrangements are not made the LAA will destroy the item after 28 days.

Why do you take this approach?

We need to ensure compliance with data protection legislation and support providers in meeting their obligations. Our guidance explains how to do this when working with the LAA.

Is this a new policy?

The new guidance document puts the spotlight on removable media. However, our approach has already been set out in data security guidance uploaded in 2018.

This followed enactment of the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA).

Looking ahead

We are currently testing two suppliers to trial alternatives to sharing data by removable media and reliance on sending USBs and CDs. Further updates will follow in 2020.

Further information

Data security requirements – for new guidance on removable media and 2018 guidance on personal data and documents