Data Handling & Deletion Procedure

PlatinumHPL
SO MUCH MORE THAN PRINT

sFTP: (SSLVPN)

We always encourage clients to send their data by sFTP.

- **Regular clients** have their own secure area to upload their data.
- **Occasional clients** are given the generic sFTP details for uploading their data.

  Using your internet Browser please browse to:

  https://upload.platinumhpl.co.uk

  Username: Platinum
  Password: Please phone for the current passwords

  Your data should have some form of identifier as the data will then be in a generic folder on our server.

Once the data is uploaded, a member of the PlatinumHPL Mailing Team is automatically notified that the data has arrived. They will then manually move the data onto the encrypted mailing server and securely delete it from the SFTP.

Emailing & USB:

If a client is not prepared to use the sFTP, they are requested to password protect their data before emailing to us and send the password by separate email or phone.

Their data should have some form of identifier as the data will be saved to a generic folder on our server.

USB Sticks:

Clients USB sticks should only be accepted if they are encypted. Clients are asked to copy their data onto our own encrypted USB.

The data will then be copied to our internal server using the procedure explained below.

Data not password protected should be avoided.

How PlatinumHPL handles your data (for information only)

Emailed data is copied to the monitored **DATA** folder on our internal server then the email is deleted. The data will automatically move to the secured part of the server.

A platinum employee will be informed the data is now in the secure folder, they will move (not copy as the data should not be left on the monitored Data folder) to the correct data folder.

Data contains:

- **Final sorted file** used in the merger, this has a sub directory data supplied which contains client supplied data that needs sorting, merging & de-duping etc.
- **Proofs** contains files sent to client for approval ie pdf/scans
- **Supplied Docs & Images** contains all files given ie word, pdf's and images etc that are to be brought into Printshop Mail, Flexmail etc.

The only file seen at first level, other than the 3 folders where information is stored, is the Printshop Mail or Flexmail etc file that the job has been printed from.

Print shop mail, flexmail or word files etc will not be placed in these sub directories.

All proofing and setup will be done from files on the server not from desktops.

Proofs will be password protected before emailing, or uploaded onto the specific sFTP (not generic).

Once approved and ready to print, they are printed direct from the server and once the job is completed the data is permanently deleted from the printer queue.

The master personalised file used to print from (including the proofs) will remain on the encrypted mailing server and will be stored in the data layer of the job folder. This will be deleted during the monthly data deletions by the assigned Platinum employee.

Monthly deletions - Every month end a platinum employee will go through and delete all data on the encrypted server from the prior month and at the same time check there is no data left on the SFTP or the switch. Data deletion is easily done by searching the mailing directory for all .csv, .mdb, .xls, .xlsx .pdf files (visual checks are done that these are customer data files). Shift delete will be used or the computer's 'recycle bin' will be emptied.

An outlook reminder will prompt them to do this, once completed the date of completion is kept in the mailing data deletion file log which is the responsibility of the mailing supervisor.

The Information Security Management System Manager, will check the data deletion file log once a month as part of the ISO27001 audit.

Returning Data

Customers requiring their data to be sent back to them would be handled in the same secure manner. Data will only be returned to the same person that sent the data. If the data is requested from another person within their organisation conformation must come from the original sender and a copy of the request (email) will be attached to the job instructions on our server.

Data will never be sent to someone outside their organisation.

This procedure has been approved by:-

Marina Wyvill
Information Security Management System Manager