BDR

BRISTOL DATA RECOVERY

SAMPLE DIGITAL FORENSIC REPORT

Was company data moved to a personal cloud account?

SCENARIO	**Suspected export of shared-drive content and a company mailbox to a personal account**
INSTRUCTED BY	**A marketing and communications agency (anonymised)**
DEVICE	**Windows 11 business laptop, 512 GB NVMe drive**
PERIOD EXAMINED	**1 May to 12 June 2026**
METHOD	**Full forensic image of the drive, analysed with our forensic software**

Sample report: anonymised, details changed. This is an example of our reporting, based on real casework. Names, dates, file names and identifying details have been changed. It is not a live case file.

CONTENTS

01 Summary of findings
02 Instructions and scope
03 How to read this report
04 Evidence and method
05 Lawful basis and proportionality
06 Limitations
07 The last day: 5 June
08 Shared-drive access
09 Deletions
10 Accounts and browser profiles
11 Key dates at a glance
12 The session on 9 June
13 Alternative explanations considered
14 Conclusions
15 What we would also ask for
16 Glossary of records relied on
17 About this sample report

Bristol Data Recovery
Castlemead, Lower Castle Street, Bristol, BS1 3AG

0117 332 1137
bristoldatarecovery.co.uk
Mon–Fri 9am–5:30pm

01 Summary of findings

On the account director's last day, the laptop records show a bulk export of the company Google account being requested and downloaded, a personal Google Drive being opened alongside the company one, and about 90 company files being deleted from the Desktop. Times are UK time (BST).

- **Mailbox export.** At 08:27 on 5 June 2026 the search "export whole gmail mailbox" was entered, and Google Takeout was opened five times in the company browser profile. Three archive files named `takeout-…-001.zip` to `-003.zip`, 5.6 GB in total, were downloaded between 09:52 and 10:31.
- **Personal Drive.** A second Chrome profile, signed in to a personal Google account, had a Drive folder titled "Work backup" open from 10:35 to 11:20. The three archives were deleted from Downloads at 11:24.
- **Shared drives.** Client folders on the company's shared drives were opened on the evening of 2 June, including contracts, rate cards and pitch documents for six clients. Opening a file is not the same as copying it, and most of this access is consistent with normal work.
- **Deletion.** Between 08:14 and 08:18 on 5 June, 92 files and folders (1.1 GB) were deleted from the Desktop. They can be listed by name, and 71 were recovered.
- **What was not found.** No USB storage device was connected in the final month. No other cloud-storage or file-transfer service was used.

The records support the conclusion that an export of the company Google account was downloaded to the laptop on the last day (confidence: high) and are consistent with its upload to a personal Drive (confidence: medium). The Google Workspace audit log will confirm or exclude both.

02 Instructions and scope

The client is a marketing agency that uses Google Workspace. An account director was given notice of redundancy on 22 May 2026 and left on 5 June. Two clients moved their business shortly afterwards. The client asked five questions.

NO.	QUESTION	SHORT ANSWER
1	Was company data exported or downloaded in bulk?	Yes: a Google Takeout export on 5 June
2	Was it sent to a personal account or service?	A personal Drive was open immediately afterwards. Upload is not directly recorded
3	Which shared-drive folders were opened in the final weeks?	Listed in this report
4	Was anything deleted?	92 items on 5 June, most recovered
5	Was removable storage used?	No

The examination was limited to 1 May to 12 June 2026 and to the account director's Windows profile.

03 How to read this report

Every finding in this report is labelled so that a reader can see at once how much weight it carries.

LABEL	MEANING
Observed fact	Something recorded on the laptop itself. The source record is named, and another examiner working from the same image would find the same thing.
Inference	What the examiner concludes from one or more observed facts. Each inference carries a confidence level.
Unresolved	A question the laptop cannot answer. Where another source could answer it, that source is named.

Confidence levels are used as follows. **High**: several independent records agree and no reasonable alternative fits them. **Medium**: the records support the conclusion, but an alternative explanation remains open. **Low**: the records are consistent with the conclusion and no more. Findings describe actions recorded under a user account. They do not, by themselves, identify the person at the keyboard or the reason for an action.

04 Evidence and method

Exhibit. One Windows 11 Pro laptop with a 512 GB NVMe solid-state drive. It was received on 15 June 2026. The client disclosed that its office manager had switched the laptop on once, on 9 June, to look for a client file. That session is identified and excluded below.

Imaging. The drive was removed, connected through a hardware write-blocker and imaged in full, including unallocated space. The image was verified by MD5 and SHA-256 hash, and the values are held on the case file. All analysis was carried out on a verified working copy.

Analysis. The image was processed in our forensic software. The Google Drive findings were checked by reading the Drive for desktop databases directly.

Sources used.

- Chrome history, downloads and profile records for each of the two browser profiles.
- Google Drive for desktop's local databases and logs, which list the account signed in and the items in My Drive and the shared drives, including items never stored on the laptop.
- ShellBags, Jump Lists and Office recent-document lists, which record folders browsed and files opened on the mapped `G:` drive.
- The USN change journal and Recycle Bin records for deletions.
- USB device history and the system event log.

Times. Converted from UTC to UK time, BST (UTC+1) throughout the period.

05 Lawful basis and proportionality

The laptop is the client's property and was examined on the client's written instruction for the specific questions listed above. The examination was limited to the stated period and to material relevant to those questions. Personal content found on the laptop was not read beyond what was needed to classify it, and is reported by category and count, not reproduced. The client was advised to record its lawful basis for the examination and to keep this report confidential to those who need it, in line with the Information Commissioner's guidance on monitoring workers. The individual concerned may be entitled to request a copy of personal data held about them, including in this report.

06 Limitations

- **Uploads are not logged by the browser.** Chrome records pages visited and files downloaded. It does not record files uploaded through a web page. An upload to a personal Drive is inferred here from timing.
- **The contents of the export are not known.** The three archives were deleted and their space had been reused before imaging, so they could not be recovered. Their names and sizes survive. What Takeout was asked to include is recorded by Google, not by the laptop.
- **Shared drives need care.** When any member of a shared drive deletes a file, the deletion appears in every member's local Drive database. A deletion record on this laptop does not show that this user made the deletion.
- **One later session.** The laptop was used for 14 minutes on 9 June by the client's office manager. Records from that session are identified and excluded.
- **A person is not identified.** The records show activity under one Windows account and two browser profiles.

07 The last day: 5 June

The account director was due to hand the laptop in at midday.

TIME (BST)	EVENT	SOURCE
08:09	Laptop switched on and unlocked by password	Event log
08:14 to 08:18	92 files and folders deleted from the Desktop, 1.1 GB	Recycle Bin records; USN journal
08:19	Recycle Bin emptied	USN journal
08:27	Google search "export whole gmail mailbox"	Chrome history, company profile
08:28 to 08:41	Google Takeout opened five times	Chrome history, company profile
09:52 to 10:31	`takeout-…-001.zip`, `-002.zip` and `-003.zip` downloaded: 2.0, 2.0 and 1.6 GB	Chrome downloads; USN journal
10:35	Second Chrome profile opened. Page title "Work backup - Google Drive"	Chrome history, personal profile
10:35 to 11:20	The same Drive folder stays open. No other browsing in either profile	Chrome history
11:24	The three archives deleted from Downloads, bypassing the Recycle Bin	USN journal
11:31	Chrome's personal profile signed out and removed	Chrome profile records; USN journal
11:46	Laptop shut down	Event log

OBSERVED FACT

The download records give Google's Takeout download address as the source of all three archives. The archive names carry the date of the export request, 5 June 2026.

OBSERVED FACT

The personal Chrome profile was created on 14 April 2026 and removed at 11:31 on 5 June. Its history database was recovered from unallocated space and covers 28 May to 5 June.

INFERENCE

A Takeout export of the company Google account was requested, downloaded and then deleted from the laptop within three hours. Confidence: high.

INFERENCE

The 45 minutes spent on a personal Drive folder named "Work backup", with no other activity, directly after 5.6 GB had been downloaded, is consistent with the archives being uploaded to that folder. An upload of that size would take about that long on the office connection. Confidence: medium.

UNRESOLVED

What the export contained: mail only, or Drive, contacts and calendar as well. Google's audit log records each Takeout request and the products included.

08 Shared-drive access

The laptop reaches the company's Google Drive through the Drive for desktop app, which presents it as drive `G:`. The table lists the client-related folders opened in the final fortnight.

DATE AND TIME	FOLDER OR FILE ON G:	SOURCE
26 May, 14:10	`Shared drives\Clients\[Client A]\2026 retainer`	ShellBags
29 May, 11:32	`Shared drives\Clients\[Client B]\Pitch June` and `Pitch_deck_v4.pptx`	ShellBags; Office recent list
2 June, 19:41 to 20:26	`Shared drives\Clients`: folders for Clients A to F opened in turn	ShellBags
2 June, 19:48	`[Client A]\Contract\MSA_signed.pdf`	Jump List
2 June, 19:55	`[Client C]\Commercial\Rate_card_2026.xlsx`	Office recent list
2 June, 20:11	`Shared drives\New business\Pipeline_Q3.xlsx`	Office recent list
2 June, 20:19	`Shared drives\Finance\Client_profitability_FY26.xlsx`	Office recent list

OBSERVED FACT

The 26 and 29 May entries fall in working hours and concern the two clients the account director managed. The 2 June entries fall between 19:41 and 20:26 and cover six clients, four of which the account director did not manage, together with pipeline and profitability workbooks.

INFERENCE

The 2 June session was not routine account work. It was a review of contract, pricing and pipeline documents across the client list, made after notice had been given. Confidence: medium. Opening a file from Drive does not copy it anywhere, and the laptop holds no record of these files being saved outside `G:`.

UNRESOLVED

Whether any of these files was downloaded, shared with an outside address or copied within Drive. The Workspace Drive audit log records views, downloads, copies and sharing changes for every file.

09 Deletions

CATEGORY	ITEMS	RECOVERED
Client presentations and proposals	31	27
Spreadsheets, including two rate cards and a contact list	14	12
Images, video and design files	29	18
Personal documents, including a CV and a redundancy calculation	11	8
Folders	7	6

OBSERVED FACT
The Recycle Bin's index records survived the emptying and give the original name, location, size and deletion time of all 92 items. Seventy-one were recovered in full from unallocated space and have been supplied to the client.

OBSERVED FACT
Every one of the 60 recovered work files also exists on the company's shared drives. No company record was lost through these deletions.

INFERENCE
The deletions are consistent with clearing a Desktop before returning a laptop. Because the company held copies of everything, they did not deprive the company of data. They are reported because the client asked, and they do not by themselves indicate concealment. Confidence: medium.

10 Accounts and browser profiles

The client asked us to be clear about which account did what, because two Google accounts were in use on the laptop.

PROFILE OR ACCOUNT	IDENTITY	USED FOR
Windows account	The account issued to the account director. Password logon only	All activity in this report before 5 June, 11:46
Chrome, company profile	The account director's company Google Workspace address	Company mail, Drive, calendar, and the Takeout pages on 5 June
Chrome, personal profile	A personal Google address in the account director's own name. Created 14 April, removed 5 June	Personal mail, a job-search site, and the "Work backup" Drive folder
Google Drive for desktop	Signed in with the company address only	The mapped `G:` drive
Windows administrator account	The client's IT provider	Software updates on 12 May. Not used on any date in this report

OBSERVED FACT

The personal profile's saved-login list, recovered with the profile, holds entries in the account director's own name for a personal mail service, a bank, a supermarket and a professional networking site. No other person's details appear in either profile.

OBSERVED FACT

On 5 June the two profiles were used in alternation within the same Windows session: the company profile until 10:31, the personal profile from 10:35, and the company profile again at 11:28 to open the handover note.

INFERENCE

One person used both profiles on 5 June, and that person was the account director. Confidence: high.

11 Key dates at a glance

DATE	EVENT
14 April	Personal Chrome profile created on the laptop
22 May	Notice of redundancy given
26 and 29 May	Shared-drive access for the account director's own two clients, in working hours
28 May	First use of the "Work backup" folder title in the personal Drive
2 June, evening	Six clients' folders and two commercial workbooks opened
4 June	Handover note written, covering two clients
5 June, 08:14 to 11:46	Desktop cleared, Takeout export downloaded, personal Drive open for 45 minutes, archives deleted, personal profile removed
9 June	Office manager's 14-minute session
15 June	Laptop received and imaged

12 The session on 9 June

The system event log shows the laptop switched on at 10:02 on 9 June and shut down at 10:16. During that session File Explorer was opened, `G:\Shared drives\Clients\[Client B]` was browsed and one PDF was opened. No file was created, deleted or changed in the account director's profile. This matches the office manager's account. Every finding in this report is dated before 11:46 on 5 June and is unaffected.

13 Alternative explanations considered

- **Taking a copy of personal emails.** Staff sometimes hold personal messages in a work mailbox, and a wish to keep them is understandable. Takeout exports whole products and cannot be limited to chosen messages, so a 5.6 GB export goes well beyond personal mail.
- **An authorised handover copy.** The client confirms that no export was requested and that mailbox handover is done by its IT provider.
- **The personal Drive was open for another reason.** That is possible, and it is why the upload is a medium-confidence inference and not a finding of fact. The folder title, the timing and the absence of any other activity are what support it.
- **The 2 June session was handover preparation.** The handover note the account director did write, on 4 June, covers two clients. Six were reviewed on 2 June, together with finance and pipeline files.

14 Conclusions

QUESTION	FINDING	CONFIDENCE
Was company data exported in bulk?	A 5.6 GB Google Takeout export was downloaded on 5 June	HIGH
Was it sent to a personal account?	Timing and page titles are consistent with upload to a personal Drive	MEDIUM
Which shared folders were opened?	Six clients' folders and two commercial workbooks on 2 June	HIGH
Was the 2 June access outside normal work?	It covered four clients outside the account director's remit	MEDIUM
Was anything deleted?	92 Desktop items, of which 71 were recovered. No company data was lost	HIGH
Was removable storage used?	No device was connected in the final month	HIGH

15 What we would also ask for

Google keeps the records that will settle the two medium-confidence findings. Audit data is kept for a limited period, so these requests should be made promptly.

WHAT WE WOULD ASK FOR

The Google Workspace audit log for the account from 1 May to 5 June: the Takeout events, which list the products exported, and the Drive events, which list every view, download, copy and sharing change.

WHAT WE WOULD ASK FOR

The Workspace login log for the same account after 5 June, to confirm that access ended when the account was suspended.

WHAT WE WOULD ASK FOR

Confirmation from the client's Workspace administrator of whether Takeout was permitted for staff accounts, and since when.

Any step to recover data from a personal Google account is a matter for the client's solicitor.

16 Glossary of records relied on

RECORD	WHAT IT IS	WHAT IT CAN AND CANNOT SHOW
Jump Lists and LNK files	Shortcuts Windows creates when a file is opened	The file's path, the times it was opened and the serial number of the volume it was on. Not what was done with the file.
ShellBags	Windows' memory of folders viewed in File Explorer	That a folder existed and was browsed, including on drives no longer attached. Not the folder's contents.
USB device history	Registry keys and the Partition/Diagnostic event log	Make, model and serial of a storage device and each time it was connected. Not what was copied to it.
USN change journal	The file system's own log of changes	Files created, renamed and deleted, with times, until the journal wraps round.
Recycle Bin records	A small index file for each deleted item	Original path, size and deletion time, even after the bin is emptied in some cases.
Prefetch and UserAssist	Program-launch records	That a program ran, when, and how often.
Browser history	History, downloads and saved-login databases	Sites visited, files downloaded, and the accounts signed in. Not what was typed into a page.
Event logs	Windows' system and security logs	Power on and off, logons, and remote-desktop connections. Older entries are overwritten.

17 About this sample report

This document is a sample. It is based on employment casework carried out by our forensic team and shows the structure, depth and wording a client receives. Names, dates, file names, device identifiers and other identifying details have been changed, and findings have been adapted so that no real person or organisation can be recognised. It is not a live case file and should not be relied on as evidence of any event.

Where a report is to be used in court or tribunal proceedings in England and Wales, it is finalised on the instruction of the client's solicitor with the examiner's qualifications, a statement of the instructions received and the declaration and statement of truth required by Part 35 of the Civil Procedure Rules.

Our work follows the four principles of the ACPO Good Practice Guide for Digital Evidence and the handling guidance in ISO/IEC 27037: the original is not altered where that can be avoided, any unavoidable change is recorded and explained, a full record of the work is kept so that another examiner can repeat it, and one named examiner is responsible for the case.

To discuss an examination, call **Bristol Data Recovery** on **0117 332 1137** or visit bristoldatarecovery.co.uk. Castlemead, Lower Castle Street, Bristol, BS1 3AG.

End of sample report. Bristol Data Recovery, Castlemead, Lower Castle Street, Bristol, BS1 3AG. 0117 332 1137. bristoldatarecovery.co.uk