Data Protection Plan

Contents

Data Protection Plan

Data Protection Plan

1. Introduction

The Privacy Policy (PP) is the external policy that informs site visitors of the steps we take to protect their privacy.

The Data Protection Policy (DPP) is the internal document that explains to those people who process personal information on the society's behalf, their obligations under the applicable legislation.

This **Data Protection Plan (The Plan)** describes how we achieve the objectives of the PP and DPP but it also deals with how we handle an additional need - to protect commercial, financial and other sensitive information that is outside the scope of personal data but which has value for the Society and/or is our intellectual property.

The plan sets out the software, infrastructure, procedures and precautions that must be adopted to achieve this aim both within the Society systems and without. It describes the training that is being provided to ensure that all volunteers in the Society are able to comply with the policies.

It also describes our data resilience and backup strategy

2. Infrastructure

The Society runs a small local area network at the Centre and provides a number of standalone laptops to branches and to events to facilitate meeting presentations. However, the vast majority of the work and almost exclusively all of the personal and other sensitive data is processed by over 100 volunteers using their personal devices - the BYOD[1] principle. Thus, the Society has no control over the user environment and no way of mandating how or if those devices are up-to-date in terms of OS, AV, backups and physical security. We cannot trust BYODs and this dictates how we approach data security. If we cannot trust the device we need an environment where the content is created and stored in a protected area, segregated from the device.

3 Data and File Types

3.1 Personal data

This is any data covered by the UK General Data Protection Regulations (GDPR), as described in the Society DPP, for example membership information.

[1] Bring Your Own Device

3.2 Commercial, Financial data and content which is our Intellectual Property (Commercially Sensitive)

This is data or information not covered under the GDPR but valuable to the Society, for example, project data such as parish register transcriptions or monumental inscriptions which have a commercial value to the Society, and Financial data such as sales figures and annual accounts.

3.3 'Office' type files

These files are used:

- for the day-to-day running of all aspects of the Society
- constitute the vast majority of usage by the widest range of volunteers in the Society
- will contain all types of personal, commercial and financial data.

The BYOD platforms on which these are created and shared represent the greatest security risk.

The IT proficiency and knowledge of volunteers is understandably varied especially given our demographic, and this means precautions must be taken to protect our content. There is a heightened risk of theft, loss or corruption of files on BYODs for our demographic.

3.4 'Data' type files

These are very large data files created by specialist software, for instance

- those arising from BerksFHS Projects,
- during the compilation of The Historian
- meeting video recordings.
- society archives
- library content
- are used by a small number of users
- 'Data' type files are very unlikely to contain personal information covered by GDPR but they are of considerable commercial value to the Society and represent the majority of the Intellectual Property.

3.5 Paper Records

Paper records are in scope if they contain personal data covered by GDPR or commercially sensitive data and are subject to the same controls as digital content - the medium is irrelevant.

4. Data Security Principles

Data is secured using these principles

4.1 Need to know

Users are granted access to the data they need to complete their assigned tasks for the Society only. This is achieved by creating restricted shared drives in Google Workspace (GW) and on the Synology NAS drive (NAS); and user access rights on the website.

4.2 Society controlled platforms

We cannot control the security of BYOD so we will provide secure cloud platforms on which data is created and stored that is accessed via a browser and creates a security perimeter around the content. Data may be created and stored on platforms provided by the society only. No content is permitted on BYODs except under a small number of controlled exceptions, detailed below.

4.2.1 'Office' type files / small content sets

1. All volunteers have access to the Society's Google Workspace environment which shall be used for the creation and storage of all Society email and office type document, spreadsheets, slide decks etc using the GW equivalents of Word, Excel, Powerpoint, Outlook etc

2. The use of MS Office is only permitted in the extremely rare occasions when the GW equivalent does not have a function that is required to complete the task

3. GW shall also be the storage location for all other small data sets that are created using other applications such as a desktop graphics design app for the Historian and in these circumstances files may be synchronised with GW using Google File Stream[2]

[2] This is one of the exceptions to the ban on society content on BYOD

4. There is an upper limit of 30GB in any GW storage allocation for a user, and if inadequate, the content qualifies as a 'Data' file type'

By using GW and providing the application in the cloud we eliminate the security vulnerability caused by insecure BYODs. We also eliminate the loss of personal or commercially sensitive data stored locally on volunteers' BYODs

4.2.2 'Data' file types / large content sets

1. These are large data sets that exceed or have the capacity to exceed the GW 30GB allocation per user and are likely to use specialist software.

2. The user base for these files is small (<10) and for this group we require the user's BYOD has up-to-date OS, AV and is protected by a password. The BYOD is not joined to our domain and the responsibility for keeping it up-to-date rests with the user.[3]

3. The user is provided with an account on the Synology NAS drive and creates one or more synchronisation tasks to synchronise data stored in local folders on the BYOD to Team folders on the NAS using two-way sync for operational content and one way sync (up to server) for archive content.[4]

4. Content may be created using local copies of programs such as MS Office which must also be up-to-date but this only relates to this class of data. Those people who have access to the NAS are likely to also have a society GW account which is used for 'Office' type file (see 4.2.1)

4.2.3 Web Services

4.2.3.1 Main Society Site

1. The site uses WordPress and is administered by the Webmasters with assistance from Uniquely Yours web hosting when required, under the terms of the managed service web hosting arrangement; data controller and data processor agreement; and restricted transfers agreement

[3] Where this would require the volunteer to incur costs they would not otherwise incur, the Society would give consideration to purchasing the required computer, on a case-by-case basis and subject to Trustees' approval

[4] This is the second exception to the ban on society content on a BYOD

2. Admin access is strictly limited. All other access to the back end is on a need-to-know basis
3. The system is backed up nightly and also whenever a plugin update is actioned, locally and to the Synology NAS
4. WordPress and its plugins are kept up-to-date to minimise security vulnerabilities
5. A Security plugin is used to maximise security including functions such as brute force attack prevention, geoblocking and auto blocking
6. Uptime monitoring is provided by ManageWP
7. The site contains the following key data sets
    a. Membership (past and present)
    b. Events and bookings
    c. Forum
    d. Public and member-only data sets
    e. Journals archive (including Exchange Journals)

4.2.3.2 Shop Site

1. This site is subject to the same criteria as the main site - see items 1 - 6 in previous section
2. The site contains
    a. Products
    b. Orders
    c. Ebooks (for data downloads)
    d. Inventory

4.2.3.3 YourTrees

1. This site is self-hosted on the Synology NAS
2. It contains members family trees and is subject to Terms of Use
3. The data is backed up as part of our 3-2-1 strategy (see below)
4. Admin access is limited to Paul Barrett, Dave Osborne and Alan Brooker
5. Mods (plugins) are used to limit the indexing of data by search engines

4.2.4 Paper Records

4.2.4.1 At the Centre

1. Paper documents containing commercially sensitive information or personal details are stored in the office of The Centre for Heritage and Family History.
2. The office is fitted with an alarm system, accessible only by named keyholders and the documents are held in lockable cabinets.
3. The Centre itself is situated within a public library which is protected by an alarm when the building is closed.

4.2.4.2 In Members' Homes

1. We acknowledge that as our society is run by volunteers from their homes, paper records will exist outside the Centre.
2. Any such records:
    a. Must be kept to the minimum required to meet the immediate needs and should not be kept at all if they exist in digital form on one of the society systems
    b. Must be secured so they are inaccessible to other members of the household.
    c. Are subject to the same retention rules as digital content
    d. Must be disposed of by shredding and not in the normal paper recycling process
    e. If longer term storage is required, they should be transferred to the Centre

5. Google Workspace Implementation

GW is implemented so as to secure Society data.

5.1 Gmail

Gmail is the sole email system to be used by volunteers and is also the gateway to Google Drive, Docs, Sheets and Slides. Volunteers will be granted a Gmail account only when they have completed a Data Privacy Self Assessment and must access mail from their browser

Exception: There is a small group of extremely low interaction volunteers for whom the task of onboarding to GW is disproportionate to the content they control, and these will be allowed to use their own email service. If they begin to produce content for the Society they must migrate to a Society account

5.1.1 Personal versus Service account

Each individual is given a *personal* account in Gmail which comes with a 30GB data allowance for email and documents.

Service accounts are created for key roles such as Chairman, Vice Chairman, Treasurer, Secretary, Membership Secretary, Webmaster and IT Manager, and for each of the branches. These permanent accounts are used for content that pertains to that role, has its own 30GB data allowance and is managed day-to-day by the current incumbent. When the incumbent changes, the credentials are passed to the successor.

5.1.2 IMAP and forwarding

These functions allow email arriving at a Society email address to be forwarded to a volunteer's private email service on a BYOD. This places the data outside the security perimeter created by GW, so these services are not permitted. Where a volunteer has issues complying, the society will work with them to reach a mutually acceptable solution that brings the data within the perimeter.

5.2 GW Apps

GW Apps include Drive, Docs, Sheets, Slides. The latter three apps do not create discrete files as in MS Office (docx, xlsx. pptx). Each file is virtual - a container which comprises fragmented data elements saved on multiple servers so that an attack on one server would be unable to reach a whole document or propagate across the entire network

5.2.1 File Sharing

There is no physical file to share. Instead links are shared to the single virtual 'document.' The sharing of links instead of physical files keeps the content inside the security perimeter.

5.2.2. Sharing Externally

GW documents can be shared externally by sending a file link to the third party. The recipient will access the document using GW and a secure tunnel to the limited content. Documents should not be converted to MS Office and emailed as an attachment because that defeats the purpose of The Plan.

6. Synology NAS Drive Implementation

The main NAS provides these services:

1. Digital Archive of all society content including content formerly stored in OwnCloud[5] Active Backup of Google Workspace (see section 7)
2. Synology Drive Service to provide synced copy service of files held on users' BYODs (see 4.2.2)
3. Video server for Society recordings
4. YourTrees Web servers

[5] OwnCloud is a self-hosted cloud storage system formerly used to provide a private cloud

While volunteers using the NAS are required to have an up-to date system, an AV program (McAfee) runs as an independent service on the main NAS as an additional layer of protection

The backup NAS is purely used as a local backup device and is only accessible to the NAS admins (see below)

7. Systems Resilience and Backup

7.1 Resilience

GW resilience is a function of the Google service.

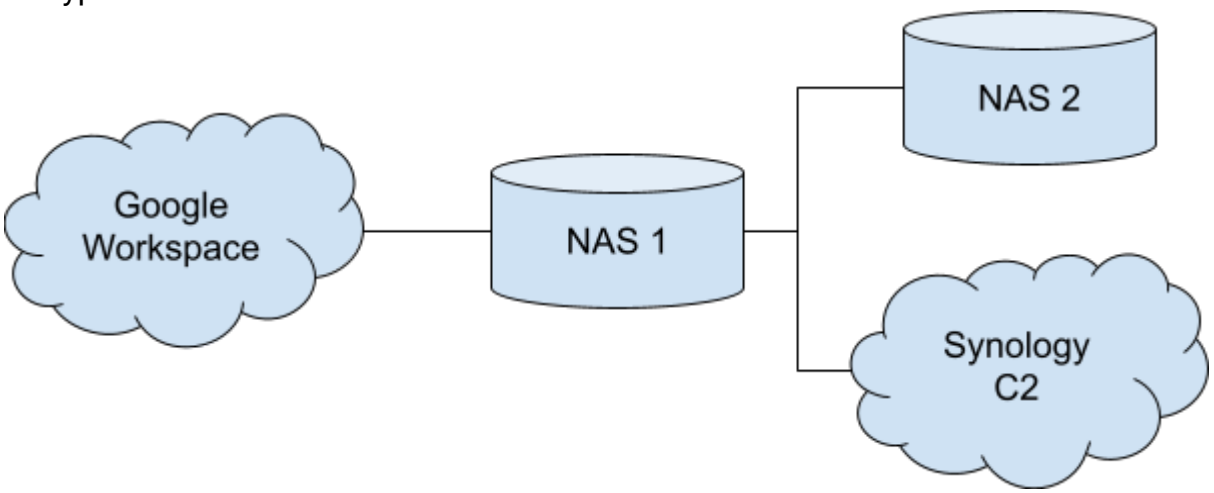
On the main Synology NAS, resilience is provided by having

- 4 HDDs in SHR-2 allowing for 2 disk redundancy (for services 1-4 in section 6)
- 2 SSDs in SHR-1 allowing for 1 disc redundancy (for service 5.)
    - There is scope to increase the SSDs to a qty of 3 in SHR-2 for 2 disk redundancy depending on the popularity of the service

The backup NAS has 2 HDDs in SHR-1 allowing for 1 disc redundancy

7.2 Backup

We use a 3-2-1 backup strategy with 3 copies of the data - the original, a second local copy for fast restore and an offsite backup using Synolog's C2 Cloud backup service, encrypted



Backups run on a nightly basis with a 180 version rotation cycle on the local copy and 256 versions on the cloud copy.

In addition the YourTrees web server, although included in the nightly backup, is locally backed up 4 hourly with a 180 version (approx 30 day) rotation.

8. System Administration

Google Workspace is administered by the IT Manager with Webmaster (Paul Barrett) as backup. The Synology NAS Drives are administered by Paul Barrett with backup from Tony Wright

It is a function of the administrators' role that they need access to all areas of the system and therefore have visibility of data which is confidential. They must work to the principle that they will access private information on computer systems only when it is necessary in the course of their technical duties. They must also maintain and protect the confidentiality of any information to which they may have access regardless of the method by which they came into knowledge of it.

9. Training

9.1 Understanding the Data Protection Policy

When they start volunteering, and annually on a fixed date, the volunteers will be requested by the Secretary to complete a Data Privacy Self Assessment in the Volunteer Information Zone section of the website, to review the latest version of the policy documents (also hosted in VIZ) and complete the online Data Privacy training courses. Progress can be monitored to ensure everyone has completed the training.

9.2 Adoption of Gmail and Google Workspace

Short training videos have been prepared on each of the following topics to help volunteers start using G Suite (the former name for Google Workspace:)

1. Team collaboration and information security
2. Accessing G Suite and the basics of *Drive*
3. Creating a G Suite document
4. Sharing files and folders
5. Uploading and converting existing content
6. Collaborating on G Suite content
7. Making it easy to access *Gmail* and *Drive*
8. The effect on share link when moving a file

9. Society wide shared files

These can be accessed via the link below. They are concise, bite-sized sessions describing how to perform common tasks

G Suite Training Videos

9.3 Advice to assist volunteers to secure their own computer devices.

An online training course is being trialled describing what volunteers should do to ensure their devices are sufficiently secure for when, for example, they upload data to Society systems. This is particularly aimed at those volunteers who will be uploading 'Data' type files to the NAS, the successful protection of which is paramount. However, it is also important that files uploaded to Google Drive are not contaminated.

10 Volunteer Action Required

10.1 Security of the Society environment

Volunteers are required to use only their allocated Society Gmail addresses when dealing with Society business (unless their interaction is rare - see 5.1). They are also required to use Google Workspace, Drive, Docs, Sheets and Slides when viewing, creating or editing documents relating to the Society.

10.2 Removal of Society information on volunteer devices.

Volunteers are required to review what Society information they have on their personal computer equipment and take the following actions:

- ☐ If they have a Google Workspace account and the content is part of the day-to-day operations of the society, upload that data to Google Workspace
  - ☐ Use My Drive for ad-hoc documents you own
  - ☐ Use a Shared Drive for documents that are part of a team effort
  - ☐ Use the option to convert all MS Office content to their Google equivalent format *and delete the MS Office versions*
  - ☐ *Delete all local content* and empty the recycle bin
- ☐ If they have a Synology NAS account and the content is part of one of the large projects, create a synchronisation task to sync the content to the NAS
- ☐ Delete all society emails from their personal email account(s)

Data Protection Plan

Approved by Trustees 12 Nov 2021

Administrative updates 04 Jan 2022 to correct number of first para of section 10 from 10.2 to 10.1 and 06 Apr 2022 to remove footnote concerning decommissioning of OwnCloud, which has been completed

Data Protection Plan

Appendix 1 - IMAP and Forwarding

Google Workspace protects our operational data by placing it inside a security perimeter. The Trustees approved the adoption of Google Workspace to gain control of the data.

IMAP and Forwarding of email places the mail, attachments and personal data outside the security perimeter and compromises data security. The Trustees were not asked for their approval of that practice. It's in direct contradiction to the objectives of Google Workspace and is discontinued.