Policy and procedure for handling Personal Audio-visual Data

Document Content Personal data pertaining to hearing and sight		**Date of Authorisation** 9 December 2019
Document Owner Data Protection Lead		**Date Last Updated** Dec 2019
Document Author Gill Russell		**Date of next Review** December 2020

Current Data Protection Team members

Data Protection Lead – Sue Winning suew@scriptureunion.org.uk 01908 856135
Database Manager – Gill Russell gillr@scriptureunion.org.uk 01908 856042

Version:	Comments:	Date:
1.0	Initial draft	03/01/2019
1.1	Updated to include personal audio data	10/04/2019
1.2	Updated to include additional references to staff and volunteer's personal devices, storage and archiving images	23/05/2019
1.3	Reformat and revision of document	28/05/2019
1.4	Update wording for Staff consent of photos to contractual. Storage recommendation updated text	15/11/2019
1.5	Consent forms moved to Procedures and linked to existing forms in the AVD Consent Form directory	25/11/2019

1. Introduction

Scripture Union (SU) holds and processes large amounts of personal audio-visual data for its own business objectives. It has legal and moral responsibilities for protecting this data so that the rights and freedoms of individuals as well as the charitable and business interests of SU are secured.

Processing of Audio-visual data (AVD) is an essential part of helping to further the work of SU. SU will ensure that all AVD represents individuals appropriately and with due respect. It will take the privacy of the individual seriously and will take all due care and consideration when handling personal data.

2. Purpose

This policy sets out how SU will process AVD of children, young people and adults in a fair and lawful way.

3. Scope

This policy applies to any form of recorded AVD of a living individual, where the individual is identifiable. It applies to the lifecycle of that data, from capture to deletion and to any person who is involved in the processing of the data on behalf of SU.

AVD covers any form of visual imaging, whether on film or in digital format, still or moving and audio recordings.

4. Responsibilities

All staff, volunteers, contractors or third parties who handle or process SU's AVD must be familiar with this policy and comply with its terms.

The Data Protection Team, comprising the Data Protection Lead (DPL) and Database Manager (DM), has responsibility for managing the implementation of this policy and procedures.

The DPL has responsibility to the Trustees for ensuring that data protection risks are managed.

5. Audio-visual Policy

5.1 Marketing/Promotion and published content

Event / Holiday – Participants and Volunteers

Where an individual is identifiable from the captured AVD, consent from the individual must be gained.

- Where the individual is 18 years or older, we will seek to gain permission from the individual.
- Where the individual is 16 or 17 years old and where the individual is able to fully understand the implications of providing consent, we will seek to gain permission from the individual.
- Where the individual is under 16 or a vulnerable adult or is not able to fully understand the implications of providing consent, the holder of parental responsibility must give consent.
- The individual must be informed of how their AVD may be used and the retention period that the data may be kept for, before giving their consent.
- The individual may remove their consent at any time.

Where an individual is unlikely to be identifiable from the captured AVD, e.g. images taken with wide angle shots or at public events, SU will use a legitimate interest basis for using this data.

- Where legitimate interest is used, information to subjects will be clearly displayed informing them that this type of recording is taking place.
- Where legitimate interest is used, a mechanism for the subject to opt out of the recordings must be made available.

School Parties

When a school sends a party of children to attend an event, SU will process the images and/or sound recordings only where the school has given permission to SU to do so, and in line with the school's own policies.

Child Safeguarding

Children's names or personal information pertaining to an audio-visual recording will not be used in captions or on SU's website.

SU will only use images of children in suitable clothing to reduce the risk of inappropriate use. SU recognises that some activities present a much greater risk of potential misuse, for example swimming and drama; under these circumstances additional care will be used in selection of the images.

Photographers / recording personnel

External professional recording personnel

Professional photographers/press must be made aware of SU's personal AVD policy and SU's expectation of them in relation to safeguarding of children.

AVD with clearly identifiable persons are personal data. As such, a third-party data processing agreement must be completed before Professional Photographers are commissioned on behalf of SU.

SU will not permit photographers to have unsupervised access to children unless verification has been received in advance that the individual has a current Disclosure & Barring Service (DBS) certificate.

Independent photographers

AVD given to SU by third parties, where individuals are identifiable, can only be used if appropriate consent has been obtained in line with this policy. The third-party checklist should be sent to the third party and returned to SU with their acknowledgement that due diligence was undertaken before the AVD was passed on to SU.

Staff/volunteer photographers

Staff should use SU devices wherever possible for recording AVD. If other devices are used, including mobile phones, the data should be handed to SU at the earliest opportunity and deleted from that equipment.

Staff and volunteers involved in holidays and events on behalf of SU may capture AVD where authorised to do so and where either relevant consent has been gained from the data subjects or legitimate interest assessments have been made.

Where an employee's or volunteer's personal device is used to capture AVD, that device should be secured for use by the authenticated user and have the latest software updates where possible. A self-audit must be undertaken at the end of a season (e.g. Christmas, Easter, summer) to ensure that personal AVD is transferred to the authorised central location for permanent storage, access and monitoring. The data should then be removed from personal devices and corresponding server locations.

Storage

AVD will be stored securely at an authorised central location. Hard copies of AVD will be kept in a locked drawer and electronic sound/images in a protected folder with restricted access.

Images/sound data will not be stored on unencrypted portable equipment (eg laptops, memory sticks and mobile phones) for longer than is necessary.

Publishing Personal Data

Every care will be taken in selecting AVD for media publishing to ensure that indecent or derogatory data is not exposed on either digital platforms or printed media. AVD may only be published where consent has been given where a person can be identified, or a legitimate interest has been deemed appropriate. Although the AVD will then be stored on an external third-party server, SU will still be deemed as the data controller and have ultimate responsibility in ensuring that the AVD is used in line with its own data protection policies.

5.2 Archiving Images

Once the specified retention period has expired for a specific purpose, the AVD should no longer be used. The procedure for archiving or removing the AVD should be followed (see Section 13).

5.3 Historical audio-visual recordings taken prior to Data Protection Law change 25th May 2018

Promotional use

Unless specific consent has been gained, SU will not use any AVD which is more than three years old (the specified timescale) for any of its promotional activity.

For AVD older than the specified timescale and where specific consent has not been gained, the data will fall into the archiving process. It will either be archived or deleted depending upon the criteria set within the archiving procedure.

The specified timescale for using AVD will continue until the data being used has specific consent, whereby this article of the policy will become redundant. The risks associated with processing this data is held within the main SU Risk Register.

Specific consent will last for the period defined in SU's Retention Policy.

Personal Devices

There should be no long-term storage of AVD captured on behalf of SU held on any personal or portable devices belonging to staff members. Any historical data should be transferred to the authorised storage area, where applicable, and removed at the earliest opportunity.

5.4 Data Subjects Rights

Request to withdraw consent / request to not have their AVD captured

Once a withdrawal of consent request has been made, the AVD must not be further processed for promotional purposes.

Where an image is recorded for legitimate business interest, if the individual makes a request to not be included in that recording, an appropriate method must be used to remove the subject from the targeted recording area. A designated safe area should be marked where individuals can have their privacy intact.

Request for Erasure

A person has a right to obtain from SU the erasure of AVD concerning him/her.

Once a request has been received, the AVD held of that person should be deleted or obscured if the conditions within Article 17 of the GDPR are met and no exemptions to this deletion are in force. *(See SU's Procedure for handling Right to Erasure Requests for more information.)*

5.5 Staff members

For security reasons, a staff member will be photographed and the image stored on SU's systems, this will be processed under a contractual basis.

If the individual volunteers for an event, as part of their volunteer application they will be asked whether they give their consent for their AVD to be captured which may be used by SU for promotion and marketing.

5.6 Visitors to our national office

For security reasons, visitors to SU's national office will be photographed for use by the security access system.

Visitors may also be photographed by our continuously recording CCTV.

6. Audio-visual Procedures

6.1 Requesting consent

A consent form must be completed by individuals attending an event confirming whether they are happy to have their AVD captured which may be used by SU for promotion and marketing. The forms can be accessed here:

- Promotions Consent Form - Child
- Promotions Consent Form - Adult

A digital copy of the consent form will be stored in the S: Media\Photo Library\Consent\<event year and name> folder along with the AVD for that event.

Volunteers applying to participate in an event or holiday through the online booking form (PAAM) will have the option to give consent at the time of booking. This option will be recorded in the Progress CRM database.

When photography is occurring but consent is not required, a notice will be displayed explaining this, giving individuals the opportunity to contact the organiser about any concerns. A template for this notice is found here:

- Promotions Photography Notice

The following checklist should be sent to a third party and returned to SU with their acknowledgement that due diligence was undertaken.

- Third Party Consent Checklist

The following checklist should be sent to schools and returned to SU with their acknowledgement that due diligence was undertaken.

- Schools Consent Checklist

6.2 Withdrawal of consent

If consent is not gained prior to the AVD being captured, the individual must not be included in any of the recording of the data. AVD should not be captured in the hope of gaining retrospective consent from the individual.

If after capturing an image an individual withdraws consent or requests removal of data from a promotion, every effort should be made to identify where that individual's data is stored and processed. If it is difficult to identify exact data items where the individual is identified, it may be necessary to restrict use of AVD within a whole folder to ensure privacy of that individual.

Third-party servers should be checked for any AVD and to the best of SU's ability, removed from these areas.

6.3 Archiving AVD

Once the retention period has expired, processing of the AVD should not continue. This data then becomes subject to the following conditions:

- AVD not required for historical purposes or legal requirements should be securely deleted.
- Holding on to the data for any other reason must be robustly documented.
- 'Just in case' is not a valid reason to retain data.

6.4 Storage

Following a review of the current structure of the photo library, the recommendation is to have a proper digital library software package that efficiently and securely stores photos and restricts access, with audit trail of who accesses photos and when. Options for this are being considered.

6.5 Staff/Volunteer self-audit

At the end of each event/holiday season (Christmas, Easter, summer) a personal data audit should be carried out to ensure AVD is removed from any device or server that has not been designated as the authorised storage location of such data.

Where the data has been captured on behalf of SU, that data should be transferred to the authorised location and removed from devices.

AVD should be deleted from portable devices such as mobile phones, laptops, memory sticks. Personal storage locations including cloud, dropbox etc should be checked and any personal data held transferred to the authorised location and then removed.

A team leader or manager should hold staff members accountable to the audit task.

7. Ownership and review

The Policy and Procedure for handling Personal Audio-visual Data is owned by DPL in conjunction with the DM. All comments, questions and requests relating to the policy and procedures should be forwarded to the DPL or DM.

This procedure will be reviewed at least annually by the DPL to ensure alignment to appropriate risk management requirements and its continued relevance to current and planned operations, or legal developments and legislative obligations.

Substantive amendments to this document need approval by the Leadership Team. Minor changes may be agreed by the DPL and DM.