Data Protection

Oaks Community Church – North East Derbyshire

Policy #	# 6
Version	v2.1
Domain	CG
Reason for update	Review after 1 year of operational experience, changes to include the provisions of the Data Protection Act (2018) and further consideration of the CCTV facilities.
Author(s)	Richard Bull

1. Purpose:

1.1 Oaks Community Church North East Derbyshire (hereafter referred to as "The Oaks") uses personal data (and occasionally 'sensitive' personal data') about living individuals for the purpose of general church administration, finance, metrics, communication and employer functions.

1.2 The Oaks recognises the importance of the correct and lawful treatment of personal data. All personal data, whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards as specified in the Data Protection Act (2018) and the General Data Protection Regulation (2016).

1.3 This policy embraces all the requirements from both Acts.

1.4 The Data Protection Act (2018) was enacted 23/05/2018 and is the legislation that brings the GDPR into UK law in preparation for when we leave the EU.

2. Need:

2.1 The Oaks needs to become better at defining its data needs, the data's longevity, assessing the legal basis for holding & processing that personal data, maintaining data security, communicating those facts to data subjects, seeking and holding a dynamic informed consent to owning and processing, ensuring accuracy and deleting time expired personal data.

2.2 The Oaks needs to become vigilant to audit its security and processes to ensure that they remain robust & fit for purpose.

2.3 Under the GDPR, data subjects are provided with a wide range of rights that can be enforced against organisations that process their personal data. It is of vital importance to understanding how new data protection law (the "GDPR") applies to the Oaks, since the penalties for ignorance are now highly punitive.

2.4 It is also important to recognise that the DPA (2018) and GDPA (2016) apply both the electronic and paper records (if systemically filed). As paper records are difficult to search (e.g. for audit or Subject Access Requests), all records will be electronic where possible, including scanning of paper documents and storing electronically.

3. Policy Points:

3.1. Data Protection Act, 2018 (DPA)

3.1.1 The Oaks fully endorses and adheres to the eight principles of the DPA. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal & sensitive personal data. Employees and any others who obtain, handle, process, transport and store personal data for The Oaks must adhere to these principles.

3.1.2 "Personal Data" is defined as any information relating to an identified or identifiable natural person, such as a name, an identification number, location data, online identifier (IP address, email address, social media details, website cookies, etc.) or to one or more factors specific to the physical, physiological, genetic, mental, economic (including: bank details), cultural, or social identity of that person.

3.1.3 "Sensitive Personal Data" is defined as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation. (Note that Criminal convictions and offences are not included under the GDPR, but similar extra safeguards apply to its processing; however, DBS checks are included.)

3.1.4 The Data Protection Principles state that data must be:

- Used fairly and lawfully
- Used for limited, specifically stated purposes
- Used in a way that is adequate, relevant and not excessive
- Accurate & kept up to date
- Kept for no longer than is absolutely necessary
- Handled according to people's data protection rights
- Kept safe and secure
- Not transferred outside the UK without adequate protection

3.1.5 The Oaks will treat all personal data as private and confidential. The Oaks will not disclose any data other than: -

- To the leadership and ministry overseers/coordinators of the church on a 'need-to-know' basis for pastoral purposes, and
- In order to facilitate the administration and day-to-day ministry of the Oaks.

All Oaks Community Church staff and volunteers who have access to personal data are required to adhere to this policy, and the Confidentiality Policy of the church.

3.1.6 There are four exceptional circumstances to the above, where information may be disclosed to outside bodies as permitted by law: -

- Where we are legally compelled to do so.
- Where there is a duty to the public to disclose.
- Where disclosure is required to protect the interest of the data subject.
- Where disclosure is made at the request or with the consent of the individual.

3.2 The General Data Protection Regulation, 2016 (GDPR)

3.2.1 The GDPR came into force 25/05/2018. It states that two main interrelated processes are required for the implementation of GDPR:
- Design of systems and processes that secure the data storage.
- Design of systems and processes that ensure that data is managed properly.

3.2.2 In particular, the GDPR requires that the Oaks have a policy concerning:
- Privacy Impact Assessments (PIAs)
- Privacy Notices (PNs) & Frequently Asked Questions (FAQs)
- Consent
- Secure data storage
- Secure data systems and processes
- Data Protection Principles (GDPR)
- Data Subject Rights
- Data Protection Impact Assessments (DPIAs)
- Subject Access Reports (SARs)
- Audits
- Breaches of data security
- CCTV

3.3 Privacy Impact Assessments:

3.3.1 Privacy Impact Assessments require the Oaks to: -
- Define our data systems and processes
- Define the data requirements for each
- Determine how long that data needs to be held (data longevity)
- Determine the legal basis for holding that data
- Consider how holding this data might affect the rights and freedoms of data subjects

3.3.2 The Oaks has six distinct data systems:
- General administration (ChurchSuite & Oaks systems)
- Finances (Oaks systems)
- Demographics & metrics (ChurchSuite)
- Communications (ChurchSuite & Oaks & TSO hosted website systems)
- Employer functions (Oaks systems)
- CCTV (Oaks systems)

3.3.3 Lawfulness: There must be a lawful basis for all processing for all types of personal data. These bases are: -
- Consent (consent only for sensitive personal data)
- Legitimate interest
- ('Exemption or derogation')

3.3.4 "Consent" means any informed, freely given, specific and unambiguous

indication of wishes by which the data subject, either by a statement or by a clear affirmative action (i.e. a positive opt-in), signifies agreement to personal data relating to them being processed. Consent cannot be inferred from silence, pre-ticked boxes, or inactivity. Consent must be separable from other written agreements, clearly presented, and as easily revoked as given. Individuals must be informed of their right to access and port data; to rectify, erase and restrict their personal data; to object to processing and, if processing is based on consent, to withdraw consent.

Consents for all storage and data processing were originally collected by form that were subsequently scanned and stored electronically.

Oaks now have the facility to collect consent electronically through registration on ChurchSuite directly via our website. Consent is not for ChurchSuite alone, but as the Privacy Notice makes clear, for all data storage and processing including images and the use of those images.

Where people object to their data and consent being stored on the ChurchSuite platform, it is still possible to collect signed paper consents and scan for secure electronic storage, as before.

3.3.5 Parental Consent - Data of Children: For the purposes of The Oaks and ChurchSuite, if consent is the basis for processing the child's personal data, a child under the age of 18 cannot give that consent themselves and instead consent is required from a person holding 'parental responsibility'.

3.3.6 The "legitimate interest" condition is intended to permit the processing of personal data for legitimate reasons, provided those interests are not overridden by the rights or freedoms of the affected data subjects (particularly where the data subject is a child). It is necessary to establish a "balance test" for processing personal data as a legitimate interest. Data controllers that rely on "legitimate interest" should maintain a record of the assessment made so that they can demonstrate that they have considered the rights and freedoms of data subjects.

3.3.7 Balance Test:

Test: Where personal data is stored or processed as a result of any of the following, then a legitimate interest is could reasonably be deemed to pertain:

- An incidental record rather than systematic use. E.g. Safeguarding notes, ministry notes, etc
- A request initiated by the data subject rather than the Oaks. E.g. Applications, reimbursements, etc.
- Data processing as a consequence of an action of a data subject rather than the Oaks, including membership and attendance at meetings. E.g. Registers, agendas, minutes & notes, gifts & donations, Gift Aid, etc.
- A request initiated by the Oaks where the purpose is to harvest opinions or views to be used at aggregate level, not the personal data itself. E.g. feedback or evaluations
- Where personal data will be stored or processed on a temporary basis for a specific episode or event and deleted thereafter, rather than kept

indefinitely. E.g. applications, permission slips, etc.

Rationale: Oaks are storing and/or processing data in a way that people would reasonably expect, without the disruption caused through seeking ***unnecessary*** consent.

3.3.8 The Oaks will seek consent for: -
- All sensitive personal data; e.g. medical information for minors (<18yr old) , DBS certificate numbers
- Personal data that is hosted on 3rd party servers (e.g. ChurchSuite & website)
- All permissions, etc. relating to minors (<18yr old)
- Photographs of both minors (<18yr old) and adults

3.3.9 The Oaks will assume "legitimate interest" for: -
- Communications regarding matters pertaining to church or "church membership"
- Processes or communications regarding requests & applications
- Registers
- Agendas, minutes and notes
- Feedback and evaluations
- Policies
- CCTV for property surveillance purposes

3.3.10 Where there is genuine difficulty in applying or interpreting the Balance Test, or where the result creates concern, the Oaks will err on the side of "consent" rather than "legitimate interest"

3.3.11 The Oaks will not rely on 'exemption or derogation' as a legal basis.

3.3.12 **Table 1: Data systems, processes, data requirements, data longevity & legal basis.**

System #1: General Administration			
Process	**Data requirements**	**Data longevity**	**Legal basis**
Church directory	Title Name Address Telephone # Mobile # Email address Household	Indefinite	Consent (Dual consent for those aged 16-18yr)
Meeting agendas	Name	Indefinite	Legitimate interest
Minutes of meetings	Name	Indefinite	Legitimate interest
Attendance registers	Name (DoB & Emergency	Indefinite	Legitimate interest

	contact mobile # for minors (<18yr old))		
Conflicts of Interest & Register of Interests	Name Interest/Conflict Name Interests	Indefinite (on minutes) Duration of interest + 1yr	Legitimate interest Legitimate interest
DBS self-declaration form	Name Address Conviction, Police investigation, allegation or cause for concern regarding conduct declaration	Until DBS results +1mth	Legitimate interest
DBS results	Name DBS certificate number	3 years + 1mth	Consent
Safeguarding notes	Name Gender	Indefinite	Legitimate interest
Approved drivers	Name Driving licence photocopy Car insurance details	Until approval period concluded (1yr max) +1mth	Legitimate interest
Booking forms	Name DoB Address Telephone # Mobile # Email address	Until event concluded +1mth	Legitimate interest
Accident forms	Name Address DoB Gender Details of accident Treatment administered Names of those in attendance	21 years	Legitimate interest
Activity Permission forms for minors (<18yr old)	Name Address DoB Parental name Telephone # Mobile # Authorised collectors Relevant medical or disability condition & medication details Email address	1yr +1mth	Consent
Medical information for minors (<18yr old)	Name Address DoB	1yr +1mth	Consent

	Gender GP name GP address GP Telephone # NHS # Relevant medical or disability condition & medication details Parental name Address Telephone # Mobile # Email address		
Image capture consents for adults & minors (<18yr old)	Name DoB Parental name	1yr +1mth	Consent
Image storage for adults & minors (<18yr old)	Name DoB Date of image Image	Indefinite	Consent
Pastoral notes	Name Address Mobile # Email address Church of attendance	Until episode concluded +1mth	Legitimate interest
SMT notes	Name Address Mobile # Email address Church of attendance	Until SMT concluded +1mth	Legitimate interest
Mentorship notes	Name	Until mentorship concluded +1mth	Legitimate interest
Feedback forms	Name	Until event concluded +1mth	Legitimate interest
Evaluation forms	Name	Until event concluded +1mth	Legitimate interest
Policies	Name Position Telephone # Mobile# Email address	Indefinite	Legitimate interest
System #2: Finances			
Process	**Data requirements**	**Data longevity**	**Legal basis**
Donations and gifts	Name Amount	Current financial year + 7 years	Legitimate interest

	Purpose		
Gift Aid declarations	Name Address	Current financial year + 7 years	Legitimate interest
Gift Aid claims to HMRC	Name Address Amount Date	Current financial year + 7 years	Legitimate interest
Legacies	Name DoB Executor's name, address, telephone #, mobile # & email address.	Until legacy received +1yr	Legitimate interest
Reimbursements	Name Amount Bank & sort code & A/C#	Current financial year + 7 years	Consent
System #3: Demographics & Metrics			
Process	**Data requirements**	**Data longevity**	**Legal basis**
Group membership	Name Email address	Indefinite	Consent
Group attendance registers	Name Apologies/reason	Indefinite	Consent
Team rotas	Name Email address	Indefinite	Consent
Location	Name Address	Indefinite	Consent
System #4: Communications			
Process	**Data requirements**	**Data longevity**	**Legal basis**
Notices	Name Address Telephone # Email address	Until event concluded +1mth	Legitimate interest
Prayer requests & updates	Name Details	Until event concluded +1mth	Consent
Letters	Name Title Address Household Additional details: - Donations (incl. Gift Aid)	Current year + 7 years	Legitimate interest
Emails	Name Email address	Indefinite	Legitimate interest
Texts & other apps	Name Mobile #	Indefinite	Legitimate interest
Dropbox	Name Email address	Indefinite	Legitimate interest
Recording of sermons	Name Date	Indefinite	Legitimate interest

	Title of Sermon		
References to 3rd parties	Name Title Address DoB Gender Attendance	Indefinite	Legitimate interest
System #5: Employer functions			
Process	**Data requirements**	**Data longevity**	**Legal basis**
Personnel files	Name Title Address Telephone # Mobile # Email address DoB NoK NI # Tax code	For duration of employment + 1 year	Legitimate interest
Attendance	Name Attendance	For duration of employment + 1 year	Legitimate interest
PAYE	Name NI # HMRC reference # Tax code	For duration of employment + 1 year	Legitimate interest
Salary	Name Bank Sort code A/C #	For duration of employment + 1 year	Legitimate interest
Appraisals	Name Date	For duration of employment + 1 year	Legitimate interest
Medical information	Name Address DoB NoK Relevant medical details	For duration of employment + 1 year	Consent
Employment checks	Name Address DoB Passport # Passport DoI/DoE Place of issue Further documents &/or details as required Professional	For duration of employment + 1 year	Legitimate interest

	certificates & qualifications		
Interview of candidates	Name Gender Address Referees Mobile # Email address Application details References Interview notes	Until appointment +1mth	Legitimate interest
Staff references from 3rd parties	Name Title Address DoB Gender	For duration of employment + 1 year	Legitimate interest
System #6: Property surveillance			
Process	**Data requirements**	**Data longevity**	**Legal basis**
CCTV		For 7 days unless specific subject data required by an appropriate authority	Legitimate interest

3.4 Privacy Notices:

3.4.1 In order for the processing to be fair, lawful, and transparent, the Oaks must make certain information available to the data subjects in the form of a Privacy Notice – a clear explanation of the Oaks' duties and their rights.

3.4.2 A Privacy Notice should be produced explaining the Oaks five "systems", viz general administration, finances, metrics, communications & employer functions.

3.4.3 Information covered should include:

- The data storage & processing principals
- The data requirements
- The processes
- Data longevity
- The Balance Test
- The legal basis for storing &/or processing that data
- The data subject's "right to object", to access (Subject Access Request – SAR) and port data; to rectify, erase and restrict their personal data; to object to processing and, if processing is based on consent, to withdraw consent.

3.4.4 Frequently Asked Questions sheet (FAQs sheet):

- The GDPR requires the Oaks to produce at least one FAQs sheet to supplement the Privacy Notice covering each process by IT system.

- FAQs are designed to provide advice in a simple Q&A format on our approaches to data storage and processing and would supplement the Privacy Notice.
- The idea is to make what the Oaks does as transparent as possible through anticipating the sorts of questions people might ask.
- The FAQ can evolve with additional questions in the light of experience.

3.5 Consent:

3.5.1 Consent forms must be separable from other written agreements, and clearly presented.

3.5.2 Where consent is the basis for storing &/or processing a child's personal data, The Oaks consider that a child under the age of 18 should not give that consent themselves (despite the fact that the DPA 2018 allows processing of data from age 13 without parental consent) and instead consent is required from a person holding 'parental responsibility'.

3.5.3 Consent forms should be kept on file for as long as the data longevity that requires the consent.

3.5.4 Data subjects have the right to withdraw consent at any time and it should be as easy to withdraw consent as to give it. Consent may relate to either the holding or processing of personal data, or both.

3.5.5 Consent should be seen as a dynamic status, and the Oaks must be able to respond to changing consent, ensuring data is only held +/or processed in line with that "current" consent status. Any data held, no longer consented to, must be securely and irrevocably deleted.

3.6 Secure data storage:

3.6.1 A fundamental element of GDPR is for organisations to evaluate the risks inherent in the processing of personal data, and implement measures to mitigate those risks.

3.6.2 Many of these risks can be mitigated by ensuring IT systems are configured to defend against cyber-attacks.

3.6.3 The GDPR requires a comprehensive IT audit is undertaken to identify all the systems and software to be assessed, including the location of equipment; network connections to external sources (internet, virtual private networks, etc.) and who owns and manages the system/s. The audit should include IP address ranges and permanent IP addresses where possible.

3.6.4 It is important to ensure that computers and network devices are configured properly to reduce the level of vulnerabilities. Changing, removing, and disabling certain default accounts, passwords and services will remove exposed weak points.

3.6.5 Firewalls should be installed to restrict inbound and outbound network traffic to services on the Oaks' internal network. The default configuration of most firewalls will not fully protect the network, so changing these default settings, such as, user names and passwords, open ports etc., is recommended.

3.6.6 Encryption of devices can provide a further safeguard against the unauthorised or unlawful processing of personal data.

3.6.7 By certifying that only authorised users have accounts and that they are only granted as much access as needed to perform their role within the organisation, will reduce the risk of information being stolen or misused.

3.6.8 Installing and updating anti-malware protection software on your devices will help detect and disable malware before it causes harm. Your malware protection should be configured to scan files automatically upon access, including removable and remote storage. Web pages should also be scanned when they are accessed through a web browser.

3.6.9 Software on your devices should always be up to date and all patches and security updates applied. This will ensure that they are not vulnerable to known security issues for which fixes are available.

3.6.10 An IT policy should cover all aspects of the Oaks' IT systems, network & devices. This should cover e.g. password management; remote access (such as VPN); mobile devices; CCTV; acquisition of new equipment, etc.

3.6.11 A culture of secured password management should be established within the Oaks office, viz: -

- Passwords of sufficient strength (length, not necessarily complexity)
- Maintaining password confidentiality
- Monthly password changes
- Plus, a change of password when staff leave (i.e. those with authorised access to the Oaks Central Server)

3.6.12 A routine back-up procedure should be maintained: -

- Daily back-ups on days the office is open (back-up data held in the safe)
- Additional weekly "fire back-ups" on a set day (e.g. Mondays), stored securely off-site

These measures will help protect against theft, hardware failure, or fire.

3.6.13 Staff Awareness Training makes staff mindful of the various cyber risks and helps create a 'security aware culture' within the organisation.

3.7 Secure data systems and processes:

3.7.1 All Oaks-related documents must be stored on the central Oaks server.

3.7.2 The only exceptions to this are:

- Paper documents/records (which should be minimised)
- Emails and texts/app based communications on personal/work IT devices.

3.7.3 There should be a data cleansing exercise across the Oaks.
- All documents relating to the Oaks should be transferred by email to the Oaks Central Server via the office and converted to the correct filename format, and stored in the appropriate folder system. ***This enables a systematic data search for SARs.***
- All duplicates on the central server should be deleted.
- All Oaks personnel (employees and volunteers) should then data cleanse their personal IT devices (PC/Mac; laptop/MacBook; tablet/iPad; smart phone) and memory repositories (memory sticks, CD-ROMs, external hard-drives, cloud facilities) of Oaks documents over 6 months old. ***This reduces the size of potential data breaches.***
- Some (e.g. Church Administrator, Group/Team Leaders, Pastoral Workers, etc) may prefer to hold some limited (***duplicate***) data on their personal IT devices for reference/continuity purposes. All with personal data on their personal devices are encouraged to keep this to the minimum they deem necessary. Where this is the case, all IT devices holding such documents should have a password access and the owner is encouraged to encrypt the device and/or activate the distant data erase facility in case of theft. ***This reduces the risk of potential data breaches.***
- Informal registers should be converted to formal electronic formats (e.g. ChurchSuite) (except fire registers, which should be paper-based and shredded after the event).
- Office based paper registers (e.g. post out/In book), could become electronic where they contain personal data.
- CCTV recordings should be held for no longer than is appropriate to allow for its specific purpose of review.

3.7.4 The “knowledge architecture” on the central server should follow a standard filename format. No two files should possess the same filename even when in separate folders.

3.7.5 Filename elements:
- Date created or relating to (YYMMDD format)
- Name relating to person, group or team
- Document type (e.g. policy, minutes, agenda, register, etc.)
- File extension (added automatically by program)

A typical filenames might be:
- 170920 Richard Bull ministry notes.docx
- 171201 Meeting Leaders minutes.pdf
- 180123 Eckington CLT minutes.pdf

3.7.6 Various personnel (both Oaks employees and voluntary staff) will produce documents in the course of their duties (e.g. agendas, minutes, policies, etc). These should be: -
- Assigned an appropriate filename, as 3.7.5 above
- Sent to the office on the distribution list for the Oaks Central Server.
- Minutes should always be shared and stored as a pdf file to avoid corruption through different versions of other formats.

3.7.7 Folders & sub-folders:
- Folders & subfolders will be filed in alphabetical order.
- Folders and/or subfolders will be protected with relevant permissions

3.7.8 A logical folder & subfolder knowledge architecture will allow appropriate filing and easy retrieval of all stored files

3.7.9 All Oaks' data processing activities should be identified. The Oaks has a responsibility to ensure its data processing activities are both secure and up to date, and where not, the Oaks should also ensure the appropriate technical and organisational measures are implemented.

3.7.10 All processes must ensure that personal data are kept confidential. This includes: -
- Positioning of computer screens such that they cannot be over-looked by office visitors.
- Time-outs/pass-word log-ins on computer screens when left unattended.
- Paper documents "re-filed" when out of the office rather than being left out on the desk.

3.8 Data Protection Principles (GDPR):

3.6.1 Data processing activities must be carried out in accordance with the Data Protection Principles set out in the GDPR; particularly, the principles of transparency and data minimisation.

3.8.2 The nature of an organisation's business and the sector it operates in is irrelevant.

3.8.3 **Privacy Notices**: In order for the processing to be fair, lawful, and transparent, the organisation must make certain information available to the data subjects, such as providing a privacy notice. However, a privacy notice by itself does not mean that processing is necessarily fair, lawful, and transparent, and other elements of fairness need to be considered, such as, using information in a way that people would reasonably expect, and thinking about the impact of processing.

3.8.4 **Purpose Limitation**: Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.

3.8.5 **Data Minimisation**: Data is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

3.8.6 **Data Accuracy**: Data controllers are responsible for taking all reasonable steps to ensure that personal data are accurate.

3.8.7 **Data Retention**: Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary and for the

purposes for which the personal data are processed. However, there are specific provisions on the processing of personal data for historical, statistical, or scientific purposes.

3.8.8 **Data Security**: Personal data must be processed in a manner that ensures appropriate security of such data, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage.

3.8.9 **Accountability**: Data controllers are obliged to demonstrate that its processing activities are compliant with the Data Protection Principles.

3.9 Data Subject Rights:

3.9.1 Identifying data subjects: Third parties might attempt to exercise a data subject's rights without proper authorisation to do so. The Oaks are required to obtain proof of identity from data subjects, before giving effect to their rights. This helps to limit the risk of third parties gaining unlawful access to personal data.

3.9.2 **Exemptions**: If the Oaks can demonstrate their inability to identify the data subject, they are exempt from complying with the data access rights.

3.9.3 **Right of Access**: Data subjects have the right to access their personal data and supplementary information via a Subject Access Request (SAR). This allows individuals to be aware of, and verify the lawfulness of, the processing.

3.9.4 **Time limits for complying with the rights of data subjects:** The Oaks is obliged to give effect to the rights of data subjects within specified time periods. E.g. This is 30 days for Subject Access Requests. Penalties for non-compliance are highly punitive.

3.9.5 **Erasure & Correction**: Data subjects have the right to correction of incorrect data and erasure of personal data (or "right to be forgotten").

3.9.6 **Restricted processing**: In some circumstances, data subjects may not be entitled to the erasure of their personal data (e.g. the exercise or defense of legal claims; protecting the rights of another person or entity; purposes that serve a substantial public interest), but may be entitled to limit the purposes for which the Oaks can process the data. **All data subject requests for erasure of information should therefore be considered against this provision before irrevocable erasure**.

3.9.7 **Right to object to processing**: Data subjects have the right to object to the processing of their personal data for the purposes of direct marketing. (This right must be communicated to the data subject no later than the time of the first marketing communication).

3.9.8 **Obligations to Inform Subjects of the Right to Object**: Data controllers are obliged to inform data subjects of their rights to object to the processing of

personal data.

3.9.9 **Right not to be Evaluated based on Automated Processing.** Data subjects have the right not to be evaluated, in any material sense, solely based on the automated processing of their personal data.

3.9.10 **Profiling**: Organisations must adhere to the strict guidelines when using automated processing of personal data. This includes having appropriate procedures, technical, and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.

3.10 Data Protection Impact Assessments (DPIAs):

3.10.1 Any proposed changes to hardware/software or systems/procedures should be assessed prior to implementation for data security.

3.10.2 Changes should only be made where the risks are understood and mitigated.

3.10.3 Generally, security improvements should result.

3.10.4 However, following some significant changes, or changes where risk actually increases, the Oaks might reasonably perform another Privacy Impact Assessment and possibly issue a revised Privacy Notice. This might necessitate a retake of consent on an updated form.

3.11 Subject Access Reports (SARs):

3.11.1 Any data Subject can request a report of all data relating to them, usually:
- Between two dates
- Regarding a particular topic
- Using other filters
- Or none

3.11.2 This applies to computer or written records (unless written records are not systematically filed), including CCTV images.

3.11.4 They have a right to information held retrospectively.

3.11.5 Information relates ***not*** to a whole document necessarily, but amounting to the key points/paragraphs relating to themselves.

3.11.6 SARs should be formatted into an electronic report for the data subject.

3.11.7 Searches should be systematically made by:
- Full name
- First name
- Called first name
- Surname
- Initials
- For CCTV images, searches will ***only*** be made where specifically requested in the SAR, and ***only*** at the site/dates/times specified. No

systematic search of the CCTV record will be made otherwise.

3.11.8 On the following IT platforms:

- Oaks central file server
- Oaks central finance PC
- Oaks website
- ChurchSuite
- Oaks employees' emails and text/app messages on Oaks IT platforms
- 'Related' Oaks volunteers (e.g. Home Group leader, other group and/or team leader) emails and text/app messages
- CCTV hard-drive recorder.

3.11.9 Identified files, emails, texts/app messages and images should be grouped into a named SAR folder with subfolders (documents, emails, texts, images).

3.11.10 A named office member should then be assigned to check the data-trawl for references to:

- The data subject (check identity if just first name, called-name and especially if initials)
- Between specified dates
- Relating to the appropriate subject enquiry

3.11.11 References should be cut & pasted into a collection template:

Filename	**Extract**
180123 Richard Bull ministry notes.docx	Ipso Lorem
180123 Eckington CLT minutes.pdf	Ipso Lorem

3.11.12 The table can then be sorted on filename to establish a chronological report.

3.11.13 The report should be read critically by a senior member of staff to determine whether 3rd party names/information should be redacted to preserve 3rd party confidentiality. Any redaction should be completed by erasure (rather than black highlighting – this can be reversed by pdf-Word conversion software) before conversion to a pdf file for sending.

3.11.14 The Oaks has just 30 days (a calendar month) to produce the report. It is for this reason that all Oaks records are held on the Oaks computer system and in electronic format in order that the full dataset can be electronically searched on filename (for scanned documents & photographs) and data subject name and initials for non-image documents.

3.11.15 The search data and report should be kept for future reference (as the same data subject has a higher probability of requesting further SARs, and this would reduce repeat search workload).

3.12 Audits:

3.12.1 The GDPR requires us to conduct regular audits but does not specify what audits we do, nor the frequency.

3.12.2 The Oaks might reasonably conduct monthly audits to check: -

- That data held is up to date
- That we do not hold data that has exceeded its data longevity
- That our systems and processes are robust and adhered to
- That our data processing is "fair" (legal and consented for)

3.12.3 Ultimately, the Oaks should be able to demonstrate from our audits that data storage and processing is:

- Stored securely
- Processed securely and fairly and legally
- Data is up to date
- Unnecessary and "time expired" data is deleted.

3.13 Data breaches:

3.13.1 Data breaches refers to any or all of:

- Breach, or potential of confidentiality
- Loss of data
- Corruption of data

3.13.2 If the Oaks becomes aware, or is made aware, of a data breach we must: -

- Re-secure the breach (hardware, software, systems/processes)
- Re-securing needs a DPIA (and potentially a new PIA, PN, re-consent)
- Inform those implicated at the earliest opportunity
- Inform the Data Controller (if significant)

References	Data Protection Policy and General Data Protection Regulations (GDPR), September 2017 by Daryl Martin, AFVS
To be read in conjunction with	#5 Confidentiality policy 2017
Specific updates from last version	Updating the Data Protection policy (16/07/17) to incorporate the GDPR
Relating policies	#7: CCTV #18: Business Continuity & Disaster Recovery Plan

Appendix 1: Privacy Notice

Introduction:

'The Oaks' is a Christian church: Oaks Community Church - North East Derbyshire.

Registered charity:	# 1115427.
A company registered in England:	# 5291244
Registered address:	2 - 4 Lea Rd, Dronfield, S18 1SB.
Phone:	01246 414448

The Oaks values everyone who engages with us by whatever means, and we do all we can to protect your privacy and to make sure the personal data you provide us is kept safe.

This policy explains how we collect data, how we use and store information and what it means for you.

We treat all in line with our beliefs and values and we welcome any feedback on any of our actions. Just call us on 01246 414448, email us at office@oakscc.org.uk or pop in in person.

The overall aim of a privacy notice is to ensure that the holding and use of personal data is fair, lawful, and transparent by giving a clear explanation of the Oaks' duties and the individual's rights.

Data collected:

The Oaks uses personal data (and occasionally 'sensitive personal data') for the purpose of:

- General church administration
- Finance
- Demographics & metrics
- Communication
- Employer functions
- Property surveillance (CCTV)

Sensitive personal data may include, but is not limited to, information relating to your physical or mental health.

We may collect personal information each time you deal with us, for example when you make a donation by gift aid, request information, sign up for an event, provide comments, complete surveys or otherwise provide your personal details we collect the information you provide.

We do not collect data from third parties.

Nor do we collect data through our website (other than for consents, registrations or bookings for events through ChurchSuite). The Oaks does not use cookies on our website, although our webhost does, and you can read their Privacy Notice at https://automattic.com/cookies/.

Consent:

Where we take consent, this can be via ChurchSuite directly, via our website, or through paper forms which are subsequently scanned and stored electronically. Consent is not simply for ChurchSuite use, but data control and processing across all our processes.

What we use the data for:

We may use the personal data we collect to:

- Keep you up to date on news and stories about our mission and work
- Ask for support, such as volunteering, prayer or financial help
- Process donations you give us
- Provide information you have requested
- Keep a record of your relationship with us e.g. questions you have asked or complaints you have made;
- Measure attendance at meetings and events
- Analyse the personal information we collect to aid our understanding of the Oaks.
- Conduct questionnaire research to aid our understanding of our church and their views.
- Provide property surveillance images if required as evidence for the appropriate authorities.

How & where we store information:

How long?

We will keep your personal information only for as long as we consider it necessary to carry out each activity. You are able to view the specifics of our policy below. We take account of legal obligations and accounting and tax considerations as well as considering what would be reasonable for the activity concerned. For example, we will retain details of donations for 7 years to meet tax and accounting requirements, but we will only hold sensitive medical personal information provided until the need to hold the information is completed.
Legacy income is an important potential source of income. We may keep data you provide indefinitely to carry out the administration of legacies.

Security:

Our data is stored in four places:

1. ChurchSuite: This is a cloud-based on-line church management system. The servers are UK-based and ChurchSuite has sophisticated, military grade security protocols and encryption of data.

2. The Oaks Central Server: This is encrypted and password protected. For security, password changes are forced monthly and with change of personnel. Connections are firewall protected and the server is backed up daily. Back-ups are stored securely and an additional weekly back-up is stored securely off-site.

3. The Oaks website: This provides information regarding our purpose, policies and activities, and lists personnel details e.g. names, email addresses, telephone numbers and images of those with various responsibilities.

4. The Oaks CCTV hard-drive recorder: This data is only accessed if needed in pursuit of evidence for the appropriate authorities (e.g. police).

We ensure that access to personal data is restricted only to those staff members or volunteers whose job roles require such access and that suitable training is provided for these staff members and volunteers.

When we share your data:

We do not share your data except by your permission.

However, we may need to pass on information if required by law or by regulatory body. For example, a Gift Aid audit by HMRC, or if asked for details by a law enforcement agency (e.g. CCTV images).

How we treat children and vulnerable persons:

All data collected on persons aged under 18 years is with parental consent.

Those without mental competence require the consent of either a Next of Kin, Legal Guardian (e.g. Power of Attorney or Court of Protection) or an Independent Mental Capacity Advocate (IMCA).

Your choices and telling us when things change:

Change of preferences:

You can change your preferences at any time on what you receive from us, or how we contact you, by writing to us.

You can do so by:
- Email us on: office@oakscc.org.uk
- Letter to us at: 2-4, Lea Road, Dronfield, Derbyshire, S18 1SB.

Updating your details:

We do appreciate it if you keep your details up to date. You can do so at any time by writing to us at the addresses above.

Telling us to stop data processing:

You have the right to ask us to erase your personal data, to ask us to restrict our processing or to object to our processing of your personal data. You can do so at any time by writing to us at the addresses above.

Your rights - the DPA (1998) & the General Data Protection Regulation (2017):

Subject Access Requests: You have the right to request details of the information we hold about you. To receive a copy of the personal information we hold please ***write by signed letter*** to us at 2-4, Lea Road, Dronfield, Derbyshire, S18 1SB stating in as much detail possible the information required: Eg.

- Date range
- Topic
- Whether specific CCTV images are required; and if so the site, specific dates and times of interest.

We will respond within 30 days of receiving your letter.

For more information about your rights under the Data Protection Act you can visit the website of the Information Commissioner's Office.

More Detail:

The General Data Protection Regulation requires us to issue this "privacy notice" to explain the data requirements of the Oaks, how that data will be stored and used, and also for how long the data will be kept for (the "data longevity").

The Oaks also needs to determine the legal basis upon which we hold that data; either that personal data requires your "consent" for us to hold and use it, or that we hold and use that data through a "legitimate interest". This is determined through a "balance test", since seeking consent for everything would be unwieldy and be unnecessary where the Oaks use that data in a way that you would readily accept and understand.

The Oaks also need to explain the principles applied in holding and using that personal data, and outline your rights.

Data Protection principles (The Oaks' responsibilities)

Privacy Notices:

In order for the processing to be fair, lawful, and transparent, the Oaks must make certain information available to you, such as providing this privacy notice. However, a privacy notice by itself does not mean that use is necessarily fair, lawful and transparent, and other elements of fairness need to be considered, such as, using information in a way that people would

reasonably expect, and thinking about the impact of use.

Purpose Limitation:

Personal data may only be collected for specified, explicit and legitimate purposes and must not be further used in a manner that is incompatible with those purposes.

Data Minimisation:

Data is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are used.

Data Accuracy:

The Oaks (the "Data Controller") is responsible for taking all reasonable steps to ensure that personal data are accurate.

Data Retention:

Personal data must be kept in a form that permits identification of "Data Subjects" (the individual whose information is held) for no longer than is necessary and for the purposes for which the personal data are used. However, there are specific provisions on the using of personal data for historical, statistical, or scientific purposes.

Data Security:

Personal data must be used in a manner that ensures appropriate security of such data, including protection against unauthorised or unlawful use, accidental loss, destruction, or damage.

Accountability:

We are obliged to demonstrate that our data using activities are compliant with the Data Protection Principles.

Data subjects' Rights (your individual rights)

Identifying data subjects:

Third parties might attempt to exercise your rights without proper authorisation to do so. The Oaks are required to obtain proof of identity from you, before giving effect to your rights. This helps to limit the risk of third parties gaining unlawful access to personal data.

Right of Access:

You have the right to access your personal data and supplementary information (via a Subject Access Request – SAR). This allows you to be aware of, and verify the lawfulness of the use.

Time limits for complying with the rights of data subjects:

The Oaks is obliged to give effect to your rights within specified time periods.

E.g. This is 30 days for a “Subject Access Request”.

Erasure & Correction:
You have the right to correction of incorrect data and erasure of personal data (the "right to be forgotten").

Restricted processing:
In some circumstances, you may not be entitled to the erasure of your personal data (e.g. the exercise or defense of legal claims; protecting the rights of another person or entity; purposes that serve a substantial public interest), but you may be entitled to limit the Oaks use of that data.

Right to object to processing:
You have the right to object to the use of your personal data for the purposes of direct marketing. (This right must be communicated to you no later than the time of the first marketing communication).

Obligations to Inform Subjects of the Right to Object:
The Oaks are obliged to inform you of your right to object to the using of your personal data.

Right not to be Evaluated based on Automated Processing.
You have the right not to be evaluated, in any material sense, solely based on the automated processing of your personal data.

Profiling:
Organisations must adhere to the strict guidelines when using automated processing of personal data. This includes having appropriate procedures, technical, and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.

Balance test

Taking consent for every time a name (or initials) is used would be burdensome and unnecessary where the Oaks use that data in a way that you would readily accept and understand.

It is therefore appropriate to determine what personal data requires “consent” to use within a particular process, and what can be assumed to be “legitimate interest”. This is intended to permit the use of personal data for legitimate reasons, provided those uses do not override by the rights or freedoms of the affected individuals.

Test: Where personal data is stored or used as a result of any of the following, then a legitimate interest could reasonably be assumed:

- An incidental record rather than systematic use. E.g. Safeguarding notes, ministry notes, etc.
- A request initiated by the data subject rather than the Oaks.
  E.g. Applications, reimbursements, etc.
- Data processing as a consequence of an action of a data subject rather than the Oaks, including membership and attendance at groups or

meetings. E.g. Registers, agendas, minutes & notes, gifts & donations, Gift Aid, etc.
- A request initiated by the Oaks where the purpose is to harvest opinions or views to be used at aggregate level, not the personal data itself. E.g. feedback or evaluations
- Where personal data will be stored or processed on a temporary basis for a specific episode or event and deleted thereafter, rather than kept indefinitely. E.g. applications, permission slips, etc.

Therefore, on balance, the Oaks will seek consent for: -
- All sensitive personal data (e.g. medical information for minors (<18yr old), holding DBS certificate numbers)
- Personal data that is hosted on 3rd party servers (e.g. ChurchSuite)
- All permissions & consents relating to minors (<18yr old)
- Photographs of minors (<18yr old) and adults.

Similarly, on balance, the Oaks will assume "legitimate interest" for: -
- Communications regarding matters pertaining to church or "church membership"
- Processes or communications regarding requests & applications
- Registers
- Agendas, minutes and notes
- Feedback and evaluations
- Policies

Where there is genuine difficulty in applying or interpreting the Balance Test, or where the result creates concern, the Oaks will err on the side of "consent" rather than "legitimate interest".

Processes covered, personal data required, the data longevity

This privacy notice covers the five data "systems" of the Oaks, and there are a number of processes undertaken in order to effectively administer the church. These are summarised in the table below, along with the personal data requirements, how long that data will be held, and the legal basis determined for holding that data as judged by the balance test:

System #1: General Administration			
Process	**Data requirements**	**Data longevity**	**Legal basis**
Church directory	Title Name Address Telephone # Mobile # Email address Household	Indefinite	Consent (Dual consent for those aged 16-18yr)
Meeting agendas	Name	Indefinite	Legitimate interest

Minutes of meetings	Name	Indefinite	Legitimate interest
Attendance registers	Name (DoB & Emergency contact mobile # for minors (<18yr old))	Indefinite	Legitimate interest
Conflicts of Interest & Register of Interests	Name Interest/Conflict Name Interests	Indefinite (on minutes) Duration of interest + 1yr	Legitimate interest Legitimate interest
DBS self-declaration form	Name Address Conviction, Police investigation, allegation or cause for concern regarding conduct declaration	Until DBS results +1mth	Legitimate interest
DBS results	Name DBS certificate number	3 years + 1mth	Consent
Safeguarding notes	Name Gender	Indefinite	Legitimate interest
Approved drivers	Name Driving licence photocopy Car insurance details	Until approval period concluded (1yr max) +1mth	Legitimate interest
Booking forms	Name DoB Address Telephone # Mobile # Email address	Until event concluded +1mth	Legitimate interest
Accident forms	Name Address DoB Gender Details of accident Treatment administered Names of those in attendance	21 years	Legitimate interest
Activity Permission forms for minors (<18yr old)	Name Address DoB Parental name Telephone # Mobile # Authorised collectors Relevant medical or disability condition & medication details	1yr +1mth	Consent

	Email address		
Medical information for minors (<18yr old)	Name Address DoB Gender GP name GP address GP Telephone # NHS # Relevant medical or disability condition & medication details Parental name Address Telephone # Mobile # Email address	1yr +1mth	Consent
Image consents for adults & minors (<18yr old)	Name DoB Parental name	1yr +1mth	Consent
Image storage for adults & minors (<18yr old)	Name DoB Date of image Image	Indefinite	Consent
Pastoral notes	Name Address Mobile # Email address Church of attendance	Until episode concluded +1mth	Legitimate interest
SMT notes	Name Address Mobile # Email address Church of attendance	Until SMT concluded +1mth	Legitimate interest
Mentorship notes	Name	Until mentorship concluded +1mth	Legitimate interest
Feedback forms	Name	Until event concluded +1mth	Legitimate interest
Evaluation forms	Name	Until event concluded +1mth	Legitimate interest
Policies	Name Position Telephone # Mobile# Email address	Indefinite	Legitimate interest
System #2: Finances			

Process	Data requirements	Data longevity	Legal basis
Donations and gifts	Name Amount Purpose	Current financial year + 7 years	Legitimate interest
Gift Aid declarations	Name Address	Current financial year + 7 years	Legitimate interest
Gift Aid claims to HMRC	Name Address Amount Date	Current financial year + 7 years	Legitimate interest
Legacies	Name DoB Executor's name, address, telephone #, mobile # & email address.	Until legacy received +1yr	Legitimate interest
Reimbursements	Name Amount Bank & sort code & A/C#	Current financial year + 7 years	Consent
System #3: Demographics & Metrics			
Process	**Data requirements**	**Data longevity**	**Legal basis**
Group membership	Name Email address	Indefinite	Consent
Group attendance registers	Name Apologies/reason	Indefinite	Consent
Team rotas	Name Email address	Indefinite	Consent
Location	Name Address	Indefinite	Consent
System #4: Communications			
Process	**Data requirements**	**Data longevity**	**Legal basis**
Notices	Name Address Telephone # Email address	Until event concluded +1mth	Legitimate interest
Prayer requests & updates	Name Details	Until event concluded +1mth	Consent
Letters	Name Title Address Household Additional details: - Donations (incl. Gift Aid)	Current year + 7 years	Legitimate interest
Emails	Name Email address	Indefinite	Legitimate interest
Texts & other apps	Name Mobile #	Indefinite	Legitimate interest
Dropbox	Name	Indefinite	Legitimate

	Email address		interest
Recording of sermons	Name Date Title of Sermon	Indefinite	Legitimate interest
References to 3rd parties	Name Title Address DoB Gender Attendance	Indefinite	Legitimate interest
System #5: Employer functions			
Process	**Data requirements**	**Data longevity**	**Legal basis**
Personnel files	Name Title Address Telephone # Mobile # Email address DoB NoK NI # Tax code	For duration of employment + 1 year	Legitimate interest
Attendance	Name Attendance	For duration of employment + 1 year	Legitimate interest
PAYE	Name NI # HMRC reference # Tax code	For duration of employment + 1 year	Legitimate interest
Salary	Name Bank Sort code A/C #	For duration of employment + 1 year	Legitimate interest
Appraisals	Name Date	For duration of employment + 1 year	Legitimate interest
Medical information	Name Address DoB NoK Relevant medical details	For duration of employment + 1 year	Consent
Employment checks	Name Address DoB Passport # Passport DoI/DoE Place of issue	For duration of employment + 1 year	Legitimate interest

	Further documents &/or details as required Professional certificates & qualifications		
Interview of candidates	Name Gender Address Referees Mobile # Email address Application details References Interview notes	Until appointment +1mth	Legitimate interest
Staff references from 3rd parties	Name Title Address DoB Gender	For duration of employment + 1 year	Legitimate interest
System #6: Property surveillance			
Process	**Data requirements**	**Data longevity**	**Legal basis**
CCTV		For 7 days unless specific subject data required by an appropriate authority	Legitimate interest

Appendix 2: Frequently Asked Questions (FAQs)

Q1: Why is some personal data held indefinitely?

A1: Because there may be a legal requirement to maintain records (e.g. Directors minutes), it provides legal protection (e.g. policies) or evidence in legal processes (e.g. safeguarding notes). In other cases, there is a historical interest or record (e.g. images).

Q2: Then why are my personal details preserved indefinitely on the Church database?

A2: Because while ever you attend this church we need those details, and should you leave, we'd like to stay in touch and keep you informed of events and so forth.

Q3: What if I don't want to be contacted after I leave?

A3: You are at liberty to exercise your right to "be forgotten", i.e. ask the Oaks to permanently erase you from the record.

Q4: What if I don't want to be erased from the record, but just don't want to be contacted?

A4: You have the right to allow us to hold your personal data but not use it. Simply let us know.

Q5: What happens if my personal details change? (E.g. email address, mobile number or address, for instance?)

A5: We have a duty to keep your data up to date, but in order to fulfill that duty, we do rely on individuals updating us on changes. Simply write to us at 2-4, Lea Road, Dronfield, Derbyshire, S181SB or drop us an email at adminstaff@okscc.org.uk

Q6: What if I suspect you hold incorrect personal data? What can I do about it?

A6: You can check this out with the office where this regards simple personal data items (e.g. email address, mobile number, bank account details, etc.)

Q7: What if I want to know more about what information you hold on me, not simply personal data items?

A7: You can ask us to provide you with the personal information we hold. This is known as a Subject Access Report (SAR). Simply request in writing the information you require, any date ranges this applies to or any subject it relates to, and we will be able to give you an electronic report of your request. We need to clarify your identity initially, but should provide you with the report within 30 days of receiving your request.

Q8: Why do we need to give consent for all the ChurchSuite functions?

A8: Because this data is held on an outside server within the UK, and although the Oaks are confident of its integrity and security, we do not control this. We therefore feel that individuals should sign a consent acknowledging this qualitative difference.

Q9: Will the Oaks always treat my personal data as confidential?

A9: The Oaks will treat all your personal information as private and confidential and not disclose any data about you to anyone other than the leadership and ministry overseers/coordinators of the church on a strictly need-to-know basis in order to facilitate the administration and day-to-day ministry of the church. All Oaks staff and volunteers who have access to Personal Data are required to adhere to the Data Protection Policy, and the Confidentiality Policy of the church.

Q10: Can the Oaks disclose my personal data without my consent? If so, in what circumstances?

A10: There are 3 exceptional circumstances where information may be disclosed to outside bodies as permitted by law:

1. Where the Oaks are legally compelled to do so.
2. Where there is a duty to the public to disclose.
3. Where disclosure is required to protect the interest of the individual concerned.

Q11: Where can I get more detail on all of the above?

A11: You can request a copy of the Oaks' Data Protection and Confidentiality policies from the office. Simply check out the 'Our Policies' page of our website (www.oakscc.org.uk) or email adminstaff@oakscc.org.uk requesting the policies you require.

Q12: Why is CCTV data not necessarily searched as part of an SAR, except if specifically requested, and with specified dates and times?

A12: This is simply pragmatic: To watch 7 days x24hrs of video surveillance from 2 sites, on 8 separate cameras would take an inordinate amount of time, possibly beyond the obligatory reply date! For this reason, anybody making an SAR will be well aware of the likely site, times and dates of interest within the last 7 days (the period for which CCTV images are held before being over-written) and should make these clear in order to reduce search time.