Dunblane Cathedral
Chris Wilson
WiFi – DunblaneCathedral Password - HallsWiFi

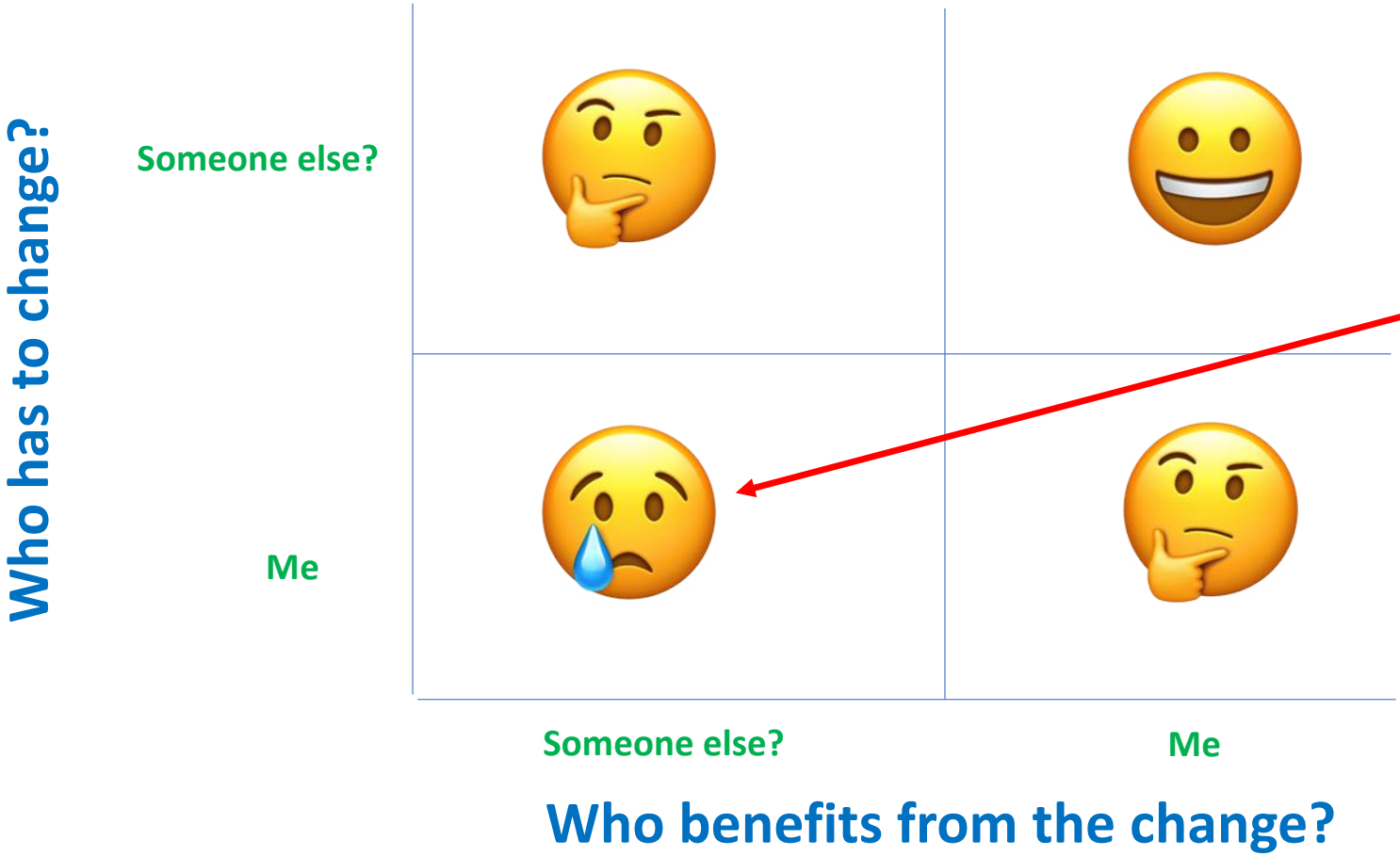
Dunblane Cathedral
Data Protection

DPO Commitment

- I will ensure:
  - our work as a church is not compromised in any way by the legal requirements placed upon us
  - We will comply with GDPR in the agreed timescale
  - We will choose technically compliant solutions to simplify how we address the legal issues
  - We will apply pragmatic and workable solutions for our Kirk Session and committees
  - Our elders/trustees, ministerial staff, employees, congregation and organisation members can rest easily knowing we are doing what is right to protect them

Dunblane Cathedral
Data Protection

Change is unpopular



Dunblane Cathedral
Data Protection

Dunblane Cathedral – A continuing journey

- **2015**
  - Decision taken to replace Dunblane Cathedral Website
  - Church of Scotland – Data Protection legal requirements to be addressed
- **2016**
  - New website and data protection requirements addressed in European-based Church Management Software – ChurchDesk chosen based on needs/demands of 21st Century church (on-line as strategy)
  - Management Committee & Kirk Session ratify investment
- **2017**
  - Management Committee & Kirk Session confirm actions and investment
  - GDPR ratified and implementation date confirmed
- **2018**
  - Management Committee and Kirk Session ratify continuation of continuing data protection strategy
  - 25 May GDPR to be implemented – Dunblane Cathedral to be compliant

Dunblane Cathedral
Data Protection

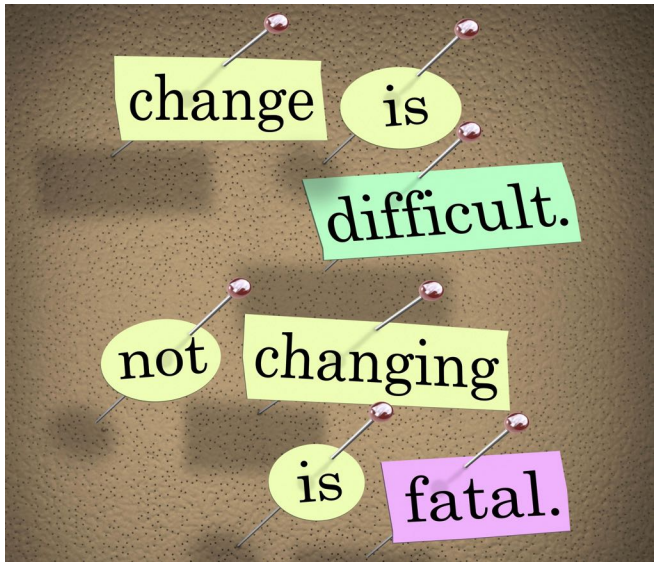
Quick Reminder

- Data Protection refers to “personal data” of living individuals – not businesses, or organisations, or other data, or if you’re dead!
- Personal Data is
  - data which relates to a living individual who can be identified –
    - (a) from that data, or
    - (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller (Stirling Presbytery and its churches), i.e. **IMPLIED**
  - and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Dunblane Cathedral
Data Protection

What is GDPR?

- **GENERAL DATA PROTECTION REGULATION** (GDPR) becomes law in all EU states on 25th May 2018
  - Replaces the current Data Protection Laws
- There are big changes which have an impact on organisations, businesses and charities
  - Elders/trustees of our churches and organisational leaders, must be aware of these changes and how they affect us



Dunblane Cathedral
Data Protection

Who benefits from GDPR?

- Every individual should welcome GDPR:
  - You are the OWNER of your personal data – name, address, email, phone number, etc. Anything which can identify you.
  - Only YOU can decide who has the right and need to hold your data
  - You have the RIGHT to be guaranteed that your data is being held securely and managed properly
  - You have the RIGHT to know that your data is only being accessed by those with a valid authority and right to do so
  - It places CONTROL of your personal data back in your hands
  - It allows you to give or remove PERMISSION for your data to be held
  - You have the RIGHT to request to view, change, or delete the data held
- We, Dunblane Cathedral, as **STEWARDS** of their data, must be able to meet those demands

Dunblane Cathedral
Data Protection

What about Brexit?

- We are still members of the EU – we must comply with all their laws until such times we leave on 29 March 2019
- 21 June 2017 - the UK Government confirmed its intention to bring the EU GDPR into UK law post Brexit
  - Data Protection Bill coming law immediately we leave - 2019
- If we share data with any part of the EU, we must comply with their data laws.
- Politically, no party will even consider making UK citizens less safe than their EU equivalents!

Dunblane Cathedral
Data Protection

GDPR – the reality

- It's the law
  - The ultimate fine for non-compliance by Dunblane Cathedral is **€20,000,000**.
  - We should be complying, not because of the fine, but because morally and legally we should be doing the "right thing"
- It's our insurance
  - It's not all "cut and dried" – some of this will be left to the courts to decide
  - We must be able to show "best endeavours"
  - We must protect our congregation, our organisations, our Church, our Presbytery and our Trustees/Elders
- Like ignoring servicing a car, we will only feel the pain when it all goes wrong!

V

Dunblane Cathedral
Data Protection

GDPR – The Details I

- **1. Personal data - enhanced**
  - The GDPR will **enhance** the definition of personal data as it will now also include identification numbers, location data and online identifiers to reflect technological advances in society.
- **2. Sensitive personal data - enhanced**
  - The GDPR will now include genetic and biometric data and will **omit criminal convictions and offences** from its definition of sensitive personal data.
- **3. Subject Access Requests – changed**
  - The rules around Subject Access Requests (SARs) will change in the GDPR. The GDPR will **remove the fee** that is chargeable under the DPA and will reduce the time limit during which we must respond to a request to **1 month**, down from the 40 days currently available. This means access to **ALL** data across the Cathedral.

GDPR – The Details II

- **4. Right to data portability – new**
  - The right to data portability will be a completely new right under the GDPR, allowing individuals to receive their personal data in an organised, **machine-readable** format.
- **5. Right to erasure – changed**
  - The GDPR will explicitly outline the **right to erasure** and will no longer require individuals to prove that the processing of their personal data caused them substantial damage or distress, which is currently a requirement under the DPA.
- **6. Record-keeping requirements – new**
  - The GDPR will place a new obligation on organisations to maintain **internal records** of all data processing activities.
- **7. Accountability principle – new**
  - The GDPR will introduce a new '**accountability principle**' in an effort to increase accountability and effective governance in data processing. (**Demonstrate** we comply)

GDPR – The Details III

- **8. Data protection by design and by default – new**
  - The GDPR will encourage a 'privacy by design' approach to data protection known as **data protection by design and by default**. This will require organisations to adopt measures that adhere to GDPR data protection principles such as data minimisation and pseudonymisation.
- **9. Data protection officer (DPO) – new**
  - The GDPR will create a new obligation for some organisations to appoint a **Data Protection Officer** who will be responsible for ensuring the organisation's compliance with the GDPR.
- **10. Penalties – enhanced**
  - The GDPR will levy **higher fines** than the DPA. Monetary fines will increase to €2,000,000 or 4% of the annual global turnover of the previous financial year (whichever is higher).

GDPR – the Principles

GDPR states, in the following 6 principles, that personal data be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
6. processed in a manner that ensures appropriate security of the personal data.

We, as Dunblane Cathedral, must "be responsible for, and be able to demonstrate, compliance with the principles."

Dunblane Cathedral
Data Protection

GDPR for Charities I

- There is no significant charity exemption to data protection or marketing law. Maybe there should be. There isn't.
- The ends never legalise the means.
- If a donor or other individual does not understand what we are doing with their personal data, the practical effect is that we can't do it, whatever it is. The same is true for consent – if a person doesn't understand what we're doing, we can't argue that they have consented to it.

Dunblane Cathedral
Data Protection

GDPR for Charities II

- We don't need consent for every use of personal data, but if we don't have consent, we need to know what other justification we have that allows us to use the data. The other reasons are specifically set out in the Data Protection Act and the GDPR.
- We cannot assume consent. Failure to opt-out is not consent. Silence is not consent. Previous support is not consent. A donation I received today is not consent for something tomorrow.
- Volunteers are no different to employees; they must be trained and equipped to protect data. There is no volunteer exemption. Using volunteers is a choice we have made, and we are responsible for ensuring that we manage the risks adequately.

GDPR for Charities III

- If we contract out any work to an agency or contractor, we are wholly responsible for what they do, unless they steal our personal data or otherwise use it for their own purposes.
- Personal data available in the public domain is still personal data and Data Protection still applies to it.
- There are specific rules for consent over the method of communicating fundraising and other direct marketing communications. Beyond that, we have to decide whether we need consent or whether some other condition applies.

"Proportionality….. something that data protection legislation is lacking in my opinion."

Dunblane Cathedral
Data Protection

What does this apply to in churches?

- Staff/payroll records
- Organisation membership lists
- Cradle Roll
- Membership roll
- Baptismal records
- Gift Aid donations
- Names on the website e.g. rotas
- Information for Pastoral Care
- Holiday clubs or activities
- Sunday schools, youth groups, crèches
- Organisation contact lists
- Digital photographs & videos where individuals can be identified

Church data is "**special category data**" i.e. sensitive like your medical data as it "*reveals a person's…religious or philosophical beliefs*"

Dunblane Cathedral
Data Protection

Legitimate Interest and Archival

- MOST data will be covered by “legitimate interest/activities” or “archival”
  - “Legitimate interest/activities” is generally how we can hold the data
  - “Archival” is how we can continue to hold data when the individual moves away
- “Legitimate Interest” means:
  - Consent has been given –it can also be withdrawn, and getting it can be fraught with issues, therefore 121 does not recommend this approach ✗
  - Processing is necessary as part of a contract e.g. staff/payroll records ✓
  - Necessary for the purposes of the legitimate interests of the church ✓
    - This is the preferred option, HOWEVER we
      - Cannot override the rights & freedoms of the individual especially if a child
      - Must identify a legitimate interest
      - Must establish that the processing is necessary
      - Must test that our interests are “balanced” with those of the individual

Dunblane Cathedral
Data Protection

Data Stewards

- We do not OWN the data
  - Holding the data does not permit us to process it any way we wish
    - Only as we have explained to the data owner
  - We MUST look after the data
    - We have been entrusted with the data
    - We must protect the data
      - Technology rather than paper
    - We must give access only to those who NEED to access the data
      - Technology rather than paper
    - We must ensure the data we hold is accurate
      - “Single source of the truth”
      - Regular verification of the data

Dunblane Cathedral
Data Protection

Implications for Dunblane Cathedral

- We MUST comply with the law as it is currently stated
  - Morally and legally, as a Church, we need to change how we hold and work with data
  - We need to embrace the changes and work together to make them successful, rather than work to avoid them
- Data Audit requirement
  - If you are holding data due to a role in Dunblane Cathedral e.g. elder, then it is Cathedral data, not personal data, and must come under the legal requirements
    - If you were not in the role would you still hold the data?
    - If you passed the data on to your successor, how would they consider the data?

Dunblane Cathedral and You

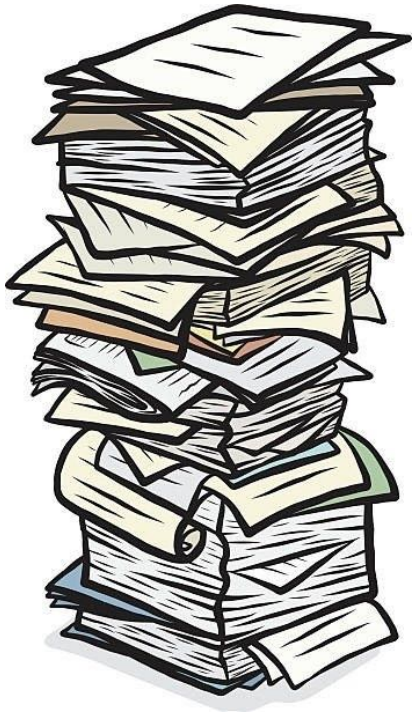
- Dunblane Cathedral has a need and a right to hold and process personal data – legitimate interest
- Being a member of Dunblane Cathedral does not give automatic access to other members' data.

- You, as yourself, do not have the right to access personal data relating to Dunblane Cathedral
- You DO have the right to access personal data relating to Dunblane Cathedral in your role within Dunblane Cathedral

Dunblane Cathedral
Data Protection

Paper Records – the GDPR Dilemma

- Basic questions **Dunblane Cathedral** needs to answer for paper records
  - Can we find all of the information we need?
    - Not only where, but can we get access across the entire Cathedral?
    - How do we allow visibility of paper records?
  - How many copies of the documents exist?
    - How up to date are they? Which is the correct copy?
  - Can we keep the documents secure?
    - How do we ensure they are only visible to the right people?
    - What do we do if the paper document gets destroyed in an accident?
    - How do we manage lost or stolen papers?
  - Can we manage our retention periods correctly?
    - How do we ensure paper is safely destroyed?
    - How do we keep paper records up to date?
    - How do we delete one person from a sheet of paper with multiple persons' details?



Dunblane Cathedral
Data Protection

Technology Benefits

- Can we find all of the information we need?
  - Yes, we can search for the data across all our technology solutions and provide it in a machine readable format
- How many copies of the data exist?
  - Generally only 1, which is the “single source of the truth”
- Can we keep the documents secure?
  - Only registered users get access to the data, and soon only to their specific data
  - Access available from any place with internet access
  - Far better backup and recovery provision than the Cathedral could manage or afford
- Can we manage our retention periods correctly?
  - Data can be marked with date/time information
  - Data can easily be deleted if required

Is it safe?

Consider: less than 100 years ago, most people kept money in paper notes “under the mattress”. Now we entrust it to a bank and technology.

Dunblane Cathedral
Data Protection

Our Strategy

- Our agreed strategy is to move from paper to technology
- Our chosen technology is the ChurchDesk Church Management Software package we invested in, for this purpose, 2 years ago
- It has never been our strategy to get rid of all paper: it is our strategy that paper can only be used where there is justifiable reason.
  - Not liking technology is not a justifiable reason!
  - Legal obligations to hold paper records are still valid
- Our policy is to adopt technology solutions unless we find insurmountable reasons which can only be addressed by paper records
  - Where paper records need to be used, they will be subject to a much more robust management process e.g. documented destruction

Dunblane Cathedral
Data Protection

Emails and ChurchDesk

- Key and public roles have Dunblane Cathedral email addresses which were moved at Easter from Google personal Gmail accounts to Microsoft business account email.
- Organisational members will be registered as users on ChurchDesk
- Users will be members of Groups e.g. Kirk Session, Choir, Handbells, etc.
- Groups will communicate, share files, and book meetings on their own Calendar

Please: do not use personal emails for Cathedral communications which contain personal information (names, addresses, etc).

Dunblane Cathedral
Data Protection

In and out… Cathedral Organisations

- Kirk Session & committees
- Cathedral Office
- Roll Keeper
- Pastoral Care
- Stewardship
- Finance
- Safeguarding
- Guild
- Handbell Ringers
- Badminton Club
- Cathedral Kids & Revelation Youth
- Change Ringers
- Choir
- Cockburn Coffee Lounge
- Connect
- Flower Diary
- Indoor Bowling

Inter data exchanges with all these organisations is fine

Dunblane Cathedral
Data Protection

In and out… Other Organisations

- Arts Guild
- Bible Society
- Boys Brigade
- Girls Brigade
- Lunch Club
- Society of Friends
- Traidcraft
- Council of Churches
- Dunblane Likhubula Partnership
- Dunblane Museum
- Guides
- Leighton Library
- Startup Stirling
- Other churches
- HRGB, etc…..

Data exchanges to these organisations need our members' consent, and those organisations need their members' consent to transfer data to Dunblane Cathedral.

Dunblane Cathedral
Data Protection

Remember…

- Anything which contains personal comments or data referring to individuals is subject to GDPR – this includes emails
- It can be extremely difficult to extract personal data from non-personal data.
  - It is therefore simpler to take a single approach to all data
- Two terms to remember: "**legitimate interests with APPROPRIATE SAFEGUARDS**" and "**archival**"
- We may have permission to hold the data, but we must do our best to keep it current and accurate

Get rid of data you don't need, or have the right to hold

- If you're not sure….ask.

Dunblane Cathedral
Data Protection

Dunblane Cathedral
Chris Wilson
Data Protection Officer

Dunblane Cathedral
Data Protection