FARRER&Co

ACF annual conference:

Preparing for the GDPR…

… and a heads up on charity law reform

Elizabeth Jones & Alan Baker

8 November 2017

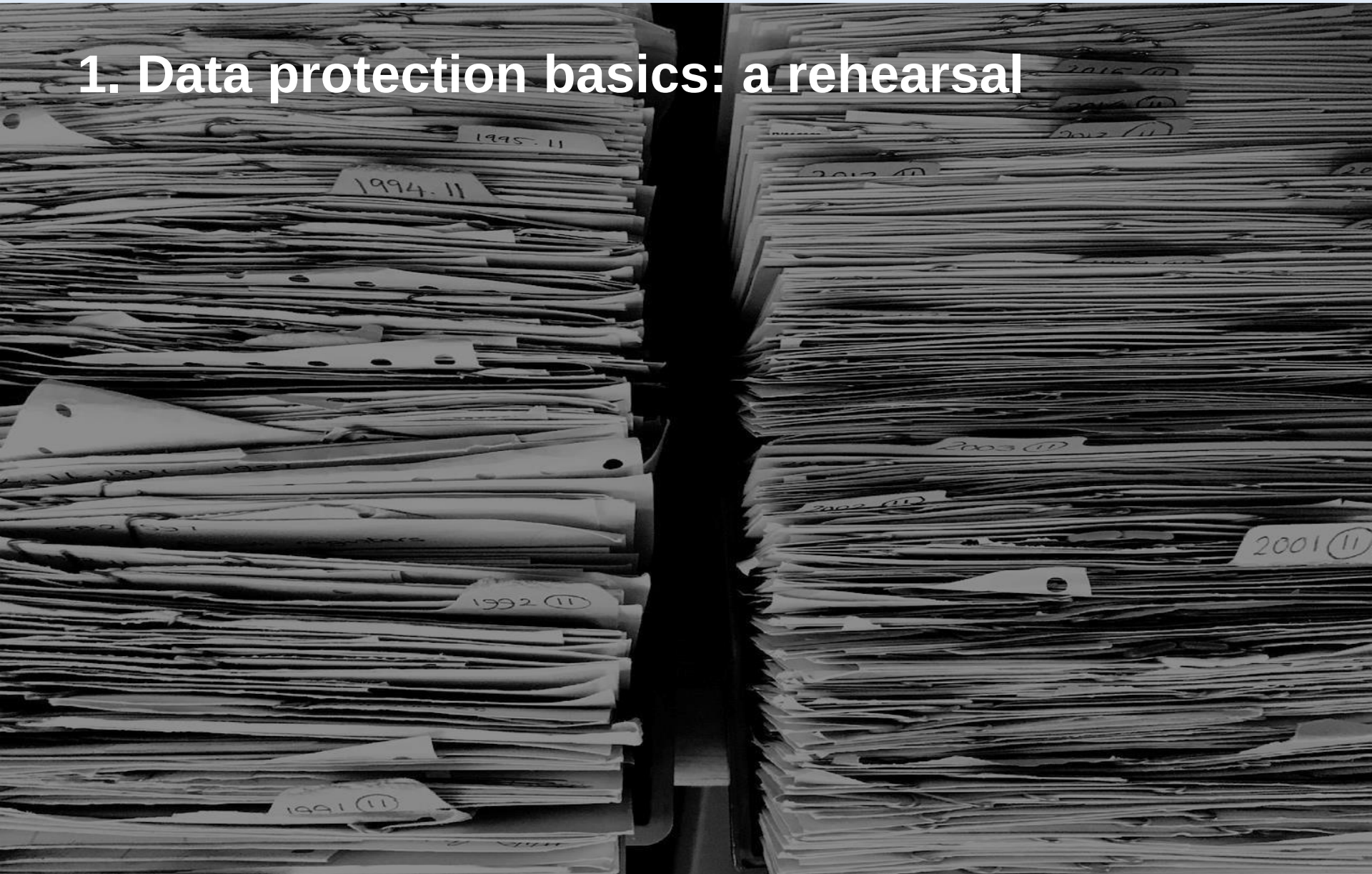
F&
Co

Agenda

1. Data protection basics: what is personal data and why does it matter?
2. GDPR: key principles, legal changes, and impact
3. Marketing: rules around 'direct marketing' and PECR
4. GDPR: key compliance steps
5. Governance: New Charity Governance Code
6. On the horizon: Technical changes to charity law

F&
Co

1. Data protection basics: a rehearsal



F&
Co

Data protection – what is it and why does it matter?

- Regulation by law of what organisations do with personal information
  - Affects anyone collecting, holding, using personal information (of living individuals) for anything other than domestic purposes
  - But also a risk – and complicated law which is changing and getting more onerous

    The General Data Protection Regulation (GDPR) goes live on 25 May 2018

  - Individuals understanding their rights, and looking to exercise them more
  - Relatively new regulator (the Information Commissioner) in-post – and she has had the charities sector in her sights
  - Fundraising Regulator also very concerned about data protection – but less relevant for this audience where ACF members are typically not fundraising(?)

F&
Co

Data protection in the headlines

- RSPCA and BHF fines in late 2016
- 11 more charities fined in early 2017

F&
Co

How it works – in headline

Data protection law basically down to this:

- Data protection principles, and in particular:
  - Fair and lawful processing
  - Data security
  - Restrictions on international transfers
- Data subject rights, and in particular:
  - Subject access rights
  - New rights under the GDPR
- Obligations on data controllers, and now under GDPR on data processors, too.
- Enforcement by the regulator (ICO) and the courts

GDPR – same framework, different and tougher rules

F&
Co

Data protection for charitable foundations (I)

- What are foundations using personal data for?
  - Processing grant applications and recording grants – sometimes made to large organisations, who themselves process large volumes of (potentially sensitive) personal data, and other times made to individuals
- As data protection legislation is principles-based, it is to be applied in a proportionate manner, bearing in mind the volume and the nature of the personal data processed by the grant-maker and/or the grantee
- Most personal data will be the grantee's, not the grant-makers – but a degree of initial due diligence, and then monitoring / evaluation may be required
- But foundations will also likely be doing some 'direct marketing':
  - Sharing updates about the foundation (for example, new funding programmes)
  - Invitations to events
  - Newsletters and bulletins, reports and research
- Potentially some fundraising, too – acknowledging this is rare for foundations

F&
Co

Data protection for charitable foundations (II)

- Are you a data controller (making decisions about how personal data is processor) or a data processor (following a data controller's instructions, assisting them with their processing) in respect of each act of processing?
- Where a data controller, what are your legal bases for processing?
  - Consent
  - Performing a contract
  - Legitimate interests
- Do you process sensitive personal data? More restrictive legal bases – and you may well need explicit consent from the data subject to do this
- Archiving of previously awarded grants may be fine but will need special care – don't just keep them mixed in with all your other data, consider access restrictions, etc. And what is the *legal* reason for keeping them?
- Keep abreast of ICO's charity-specific guidance and 'toolkits' here: https://ico.org.uk/for-organisations/charity/

F&
Co

2. General Data Protection Regulation (GDPR)

F&
Co

What is GDPR?

- Biggest change in data privacy laws for 20 years
- Pro-privacy, more accountability, tougher enforcement
- EU legislation – but affects more than just Europe
- Brexit will not prevent GDPR applying to UK – see the UK's draft Data Protection Bill (put before the House of Lords on 14 September 2017)
- 25 May 2018 is 'Zero Day' – everything must be compliant then

F&
Co

GDPR's five main themes

I. Extending the scope of EU regulation

II. Empowering individuals

III. Transparency and accountability

IV. Privacy by design

V. Sanctions for non-compliance

F&
Co

I. Extending the scope of EU regulation (1)

- Catches data controllers and data processors established in the EU

- Catches data controllers and data processors outside the EU if they process personal data in the context of:

  - offering goods/services to individuals in the EU
  - monitoring the activity of individuals in the EU

Unlikely to affect the grant-makers represented here at ACF. But please be clear: if your organisation is established in the EU, you will have to comply with the GDPR regardless of the who the personal data 'belongs to'.

F&
Co

I. Extending the scope of EU regulation (2)

- Regulation now extends to "data processors" (e.g. your cloud providers or where you are a data processor)
- Processors now have direct legal obligations backed by serious sanctions
- Controller / Processor contracts must have specific terms included in them. All new Controller / Processor contracts need to reflect this
- Remember 'Zero Day' concept – existing Controller / Processor contracts extending beyond May 2018 need to be re-negotiated

  You should certainly consider your own "data processor" agreements in good time before May 2018.

F&
Co

II. Empowering individuals (1): consent and control

- Consent must be a "*freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement*…"

- Pre-ticked boxes won't work – "Opt-in" will be the norm. Wrapping consent wording up in lengthy T&Cs won't work, either

- An individual's consent – freely given – can be freely withdrawn

- Broadly, employees cannot give consent, due to the imbalance of power in the employer – employee relationship

  - But is consent really required? Is it your 'best' legal basis for processing?

F&
Co

II. Empowering individuals (2): overview of rights

Individuals' rights in respect of their data:

- clear descriptions of processing given in plain language
- right to withdraw consent (or challenge other grounds for processing)
- right to object to the ways their data is processed: e.g. right to object to marketing, right to deletion (erasure) or correction
- right to transfer data to someone else (data portability)
- GDPR retains right of subject access (with only minor changes)

F&
Co

II. Empowering individuals (3): main impacts

- Consent may be too difficult to obtain (and too easy to withdraw) or not available at all (e.g. employees) – you need to identify why you are processing data and see if it can be justified on other grounds

- Other grounds may also be open to challenge – need to clearly explain these in advance, be prepared to justify on demand, and therefore record your decision-making

- Need new functionality / platforms to cope with / respond to enhanced rights – could mean IT systems changes

  Again this is principles-/ proportionality based – but do you have a 'defensible position', which you are happy to disclose to the ICO?

F&
Co

III. Transparency principle

- Transparency means you need to know what you do with personal data and why, from the outset, in order to explain this to individuals
- You principally explain this via new Privacy Policies / Privacy Notices
- Privacy Policies / Privacy Notices have to be clear, detailed and in plain language. They must also be 'provided to' affected individuals
- Remember 'Zero Day' – you have to do this for both new and existing contacts if you want to keep processing their data after May 2018

F&
Co

III. Accountability principle

- Accountability means not just being compliant, but being able to demonstrate compliance
- It means being accountable to the regulator (ICO) and to individuals: being able to respond promptly and properly to requests, and justify processing
- It requires careful record-keeping of the reasons for processing and the decision-making and judgment behind them
- It means being able to demonstrate that you not only have the policies and procedures in place but that they are embedded in the organisation's culture

  Again, proportionality is required – how much data? How sensitive?

F&
Co

IV. Privacy by design (1)

- This is about building privacy into systems and processes from the outset
- For example, this could affect the design and management of databases / IT systems and grant application / monitoring processes:
  - use the minimum data possible to achieve the purpose
  - is the data retained for the minimum period possible ?
  - should data be anonymised or pseudonymised ('lock and key')?
  - are security safeguards built in?
  - do employees understand this?
- An accompanying principle is 'privacy by default'; not only are your systems / processes *capable* of protection privacy – but is that their default setting?

F&
Co

IV. Privacy by design (2): main impacts

- Massive culture change within most organisations – people are the main challenge, not technology
- Led by new compliance role – the Data Protection Officer (if required – but even if no formal 'DPO' role is required, you should identify a data protection compliance lead where possible).
- Must re-assess existing systems and processes to ensure they are compliant
- Review data retention… and delete (or, at least, separate out) "risky" data
- As a minimum (for example, if you are a very small charity), at least consider your data security standards and why you are retaining any historical data

F&
Co

IV. Privacy by design (3): Privacy Impact Assessments

- Existing concept, but taking on particular importance under GDPR
- Help identify risks and steps needed – especially before new major projects or systems changes
- Also help create paper trail and record of decisions taken and why
- Useful in showing accountability and "privacy by design"

  - Again, proportionality is required – how much data? How sensitive?

F&
Co

V. Sanctions and Enforcement (1): overview

- Mandatory data breach notification
  - Controller must report to the ICO within 72 hours
  - Controller must report serious security breaches to affected individuals
  - Processor must report breaches to Controller

- Regulatory action
  - fines of up to €20M or 4% of annual worldwide turnover
  - other enforcement powers ('stop processing' notices, undertakings, audits)

How will this affect grant-making charities? Raises the risk profile for all data controllers (and data processors) but we do not expect huge fines for grant-makers based on the types / volumes of personal data they process

F&
Co

V. Sanctions and Enforcement (2): ICO priorities

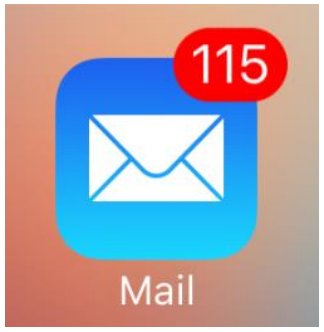
- Role and enforcement priorities of regulators:
  - Data breaches and cyber security a major focus worldwide
  - Breaches of "fair processing" an ICO target for fine
  - ICO likes Accountability – focus for GDPR enforcement

- Expect:
  - (occasional) pro-active compulsory audits in selected sectors
  - (lots of) re-active investigations after data breach reports or individual complaints

- Follow ICO guidance for indication of the particular enforcement priorities of the Information Commissioner (Elizabeth Denham). Noting this from 21 Feb 2017: "*… investigations are now complete. We are not looking at any other charities as part of our investigation into fundraising practices that were sparked by media reports in 2015. I want to draw a line under these investigations and move forward."*

FARRER&Co

3. Direct marketing



F&
Co

What is direct marketing?

- Direct marketing is defined by the Data Protection Act / PEC Regulations as: "*the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals*"
  - N.B. there is no new definition in the GDPR

- The law regulates *unsolicited* marketing; hence the importance of consent

- N.B. that direct marketing:
  - is not limited to advertising goods or services for sale (see *SNP* case from 2005 / 2006 – confirmed that the law is concerned with intrusion of individual's privacy);
  - includes sending of material promoting an organisation's "aims or ideals"

- No big changes under GDPR – although it does recognise that "*The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest*."

F&
Co

How does direct marketing become a problem?

- Individual complaints
  - Made to your organisation (causing, as a minimum, some internal embarrassment)
  - Complaints to the ICO
  - Complaints to other regulators (where relevant)

- Negative publicity
  - Off-putting for individuals your organisation relies on
  - Remember that ICO enforcement action is made public
  - You may even be subject to a press campaign, whether being singled out as a particularly bad offender or being tainted by negative press about your sector

Fundraising charities already had their (unfair share?) of media criticism, negativity and of course ICO fines. Grant-making charities generally have a lower profile but unfortunately there is some precedent for urging caution.

F&
Co

The ICO's requirements for marketing (1)

- In many cases, organisations will need consent to send people marketing, or to pass their details on. Organisations will need to be able to demonstrate that consent was knowingly and (under the GDPR) "unambiguously" given, clear and specific, and should keep clear records of consent of what an individual has consented to (and not consented to), and when and how this consent was obtained, so that they can demonstrate compliance in the event of a complaint (Accountability principle)

- ICO's current direct marketing and PECR guidance says that organisations should use **opt-in boxes** where possible. ICO GDPR consent guidance confirms this – and effectively spells the end of the 'opt-out box'

- Organisations must carry out **rigorous checks before relying on indirect consent** (i.e. consent originally given to a third party)

F&
Co

The ICO's requirements for marketing (2)

- The rules on electronic direct marketing (calls, texts, emails) are stricter than those on mail marketing. The ICO's view is that "*consent for **electronic** marketing messages is more tightly defined than in other contexts, and must be extremely clear and specific*."

- **Screen** against the TPS and MPS (the latter is not a legal requirement)

- **Stop** sending marketing messages to any person who objects or opts out

- **Don't** make automated pre-recorded marketing calls without specific consent

- **Don't** send marketing texts or emails to individuals without their specific consent. N.B. the ICO says the 'soft opt-in' rule is not available for charities

F&
Co

Enforcement (including the ICO's priorities in 2017)

- The ICO can take enforcement action wherever the law relating to direct marketing is not being complied with. Any breach of the DPA or PECR could result in an Enforcement Notice (EN), requiring an organisation to take action to remedy the breach. Failure to comply with an EN is a criminal offence.
- The ICO can also impose civil monetary penalties (fines) of up to £500,000 for a serious breach. And maximum fines much higher under GDPR.
- ICO has identified its priorities for enforcement of these rules: "*Most likely to take such action where an organisation **persistently ignores** people's objections to marketing calls or texts, sends mass texts without consent, or fails to screen its call list against the TPS*."

We fully expect that this will remain an ICO priority under GDPR. So this might well become an area for inclusion (if not to focus on – again depending on the type / volume of data processed) as part of your due diligence on grantees

F&
Co

4. GDPR: Key compliance steps

F&
Co

GDPR – what you should be doing now (I)

1. Transparency. Tell people what you are doing with their personal data
2. Training. Make sure your staff are adequately trained, including about GDPR
3. User-level data security. Use strong passwords. (E.g. not "p455word" (!))
4. Systems-level data security. Encrypt all relevant portable devices
5. Data retention. Only keep people's information for as long as necessary

These five points are the ICO's "*top five of data protection tips for small and medium sized charities and third sector organisations*". Note the focus on data security and avoiding data breaches – prevention is better than cure.

F&
Co

GDPR – what you should be doing now (II)

6. Consider data protection due diligence on grantees. Decide the level of data protection related due diligence is required as part of the grant-making process – sensitive to the nature and volume of the grantee's personal data

7. Trustee accountability. Ensure that trustees are sufficiently informed about GDPR compliance risks and involved in key compliance decisions

8. Assess legal bases for processing. Conduct a 'mini audit' and identify your legal bases for processing personal data (consent, performing a contract, legitimate interests, etc.) – and refresh privacy notices / consents as required

9. Update data processing agreements. Having considered DC / DP distinction

10. Review policy and procedure, e.g. procedures for answering SARs

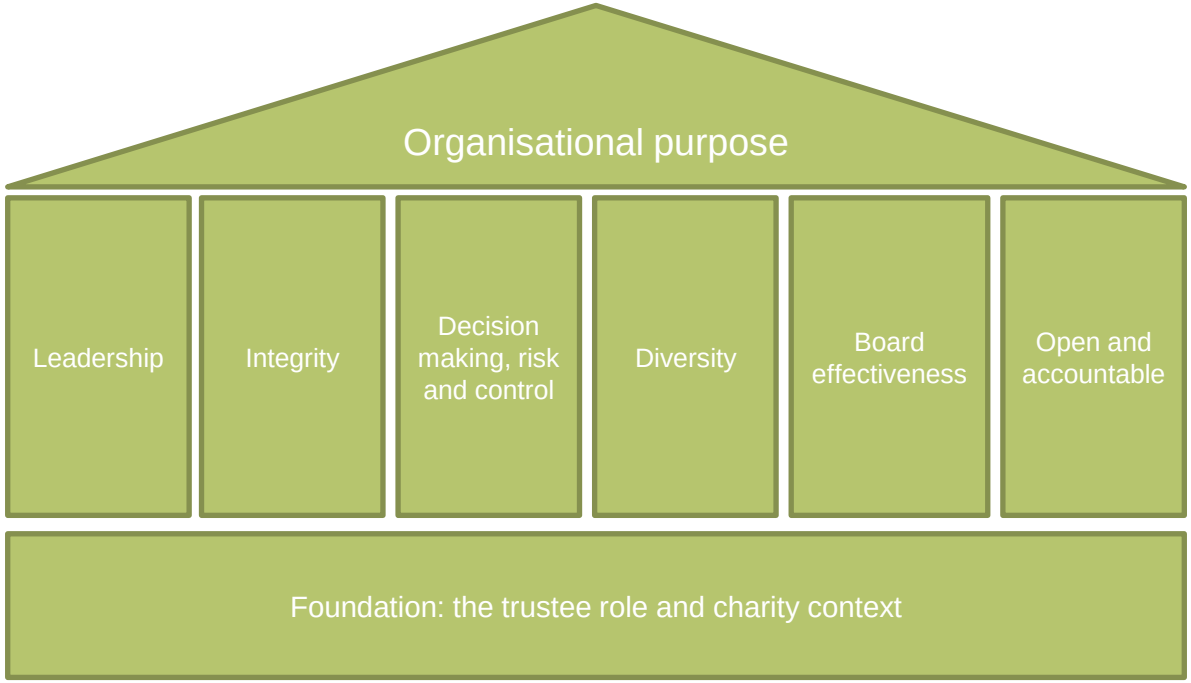
F&
Co

Charity Governance Code: Background

- Voluntary sector governance code first published in 2005, revised in 2010
- Updates reflect developments in Corporate Governance and changes in the third sector
- Developed by the Code Steering Committee comprising an independent chair and a number of leading umbrella bodies
- Draft Code issued in November 2016 for consultation
- Final version of the new Code was published in July

F&
Co

Charity Governance Code: Principles



F&
Co

New Charity Code of Governance

Key questions for trustees of larger foundations emerging from changes to the Code – do we:

- *consider the benefits of partnership working?*
- *have a code of conduct for trustees?*
- *regularly review governance structures and procedures?*
- *review matters we have delegated on a regular basis and what decisions are reserved to trustees?*
- *publish the process for setting staff remuneration?*

Will we follow an 'apply or explain' approach to the Code?

F&
Co

Law Commission Report and Charities Bill

- "Technical Issues in Charity Law" - September 2017
- Extensive consultation in 2015 and followed up last year with a supplementary consultation
- Law Commissioner, Nick Hopkins: "*As it is, some of the technical law around charities is inefficient and unduly complex*"
- Reforms are aimed at balancing deregulation against proper protection of charity assets – removing some of Lord Hodgson's barnacles on the ship

F&
Co

Ten key features

1. Aligning the rules for amending the objects of corporate and unincorporated charities

2. New broad power to amend the governing documents of unincorporated charities

3. Increasing flexibility to make ex gratia payments up to £20,000

F&
Co

Ten key features

4. Simplifying the rules on disposing of charity property

5. Making mergers and incorporations simpler

6. New powers for the Charity Commission on charity names and determining trusteeship

F&
Co

Ten key features

7. Statutory power for (some) Royal Charter bodies to amend their charters

8. Removing the provisions on special trusts

9. Simplifying the regime for failed charitable appeals

10. Nothing on public benefit or fundraising regulation!

F&
Co

Questions?

F&
Co

Thank you for your attention. Please do get in touch with any queries.

Elizabeth Jones, Partner
Email: elizabeth.jones@farrer.co.uk
Telephone: 020 3375 7138

https://www.farrer.co.uk/people/lizzie-jones/

Alan Baker, Associate
Email: alan.baker@farrer.co.uk
Telephone: 020 3375 7441

http://www.farrer.co.uk/people/alan-baker/