ANNEX A: Summary of Responses to Consultation on Data Protection in the Code of Fundraising Practice

This paper summarises amendments proposed in response to comments received from the consultation. Specific amendments to the new Code wording in recognition of points raised by respondents are outlined in **red** in the boxes.

The following themes were identified in responses to the Consultation to date.

1. General comments

Fundraising Regulator's role on Data Protection

Some respondents took the view that minimal detail on Data Protection should be provided in the Code as the role of the Fundraising Regulator should not be to produce data protection guidance or interpret GDPR.

Response
We appreciate that there is a balance to strike between those fundraisers who want specific detail on how GDPR relates to fundraising and those who feel more confident in working with the existing generic ICO guidance and GDPR. For this reason, we have focused on those aspects of data protection law that most commonly apply to fundraising.

We are clear in our Memorandum of Understanding with the ICO that we will be guided by the ICO as the statutory regulator on data protection.

Guidance for different audiences

Several respondents highlighted the differing levels of data protection knowledge in charities accessing the Code. They advocated that the Code include appropriate signposting or additional resources that will help understanding at all levels.

Response
The Fundraising Regulator is currently developing guidance with the IoF to highlight key data protection concerns for specific types of fundraising. It also intends to discuss the issue of any additional guidance that may be required for smaller fundraising charities in a roundtable event with smaller organisations in early 2018.

Legal Appendices on Data Protection

Some respondents noted that the legal appendix 14 would need updating / amending to reflect GDPR. One respondent suggested that the legal appendices should be incorporated within the main body of the Code as they risked being overlooked.

Suggested remedy
The Fundraising Regulator proposes to replace the current legal appendices on Data Protection with links to ICO guidance.

We will consider the case for greater alignment of the legal appendices as part of our Code review in 2018.

Communicating changes
Alongside communicating the changes in emails or bulletins, several organisations said they would like to see the Fundraising Regulator continue its engagement with the sector to talk about the changes and help people understand what they need to do to comply through events and other learning opportunities.

Suggested remedy
The Fundraising Regulator proposes to include data protection and the Code in its speaking engagements over 2018 and talk to the IoF and other stakeholders to identify suitable opportunities to disseminate the changes.

2. Specific issues identified

Section 3.1.1: Age Limits and Permissions

While rule 3.2.1 currently states that "many organisations view the age of capacity as 12", some respondents noted that the GDPR specifies that the minimum of age for consent to processing personal data for certain purposes should not be lower than 13. They asked that this age minimum be considered for inclusion in this section.

Suggested remedy

The current proposed wording is as follows:

3.2.1 Age Limits and Permissions

a) Organisations MUST* get explicit parent or guardian consent to collect data until children have capacity to give fully informed consent themselves. Many organisations view the age of capacity as 12, however, no definitive age is set out in legislation and whether consent is needed may depend on the context in which data is being collected/used.

b) Any information collected from anyone under 14 years of age MUST NOT be disclosed without consent from a parent or guardian.

Section 5: Personal information and Fundraising includes further information on requirements relating to data protection.

The Fundraising Regulator proposes to change this to incorporate the language of the GDPR as follows:

3.2.1 Age Limits and Permissions

Organisations **MUST*** get explicit parent or guardian consent to ~~collect data~~ process the personal data of a child until the child has capacity to give fully informed consent themselves.

*See **Section 5: Personal information and Fundraising** for further information on what "processing" means and requirements relating to data protection.*

We propose to also add an additional line to draw fundraisers attention to what the GDPR guidance in outline best practice guidance:

There is no minimum age of consent set out in legislation for general data processing activities. However, as a guide in developing their wider policies on consent, fundraising organisations should take into consideration that the GDPR requires a minimum age of consent of 13 years old to process personal data for the provision of information society services (ie a service provided for remuneration, at a distance using electronic means at the request of the individual).

Section 5.1.1: impending legislation - Data Protection Bill and future changes to the Privacy and Electronic Communications Regulations 2003 (PECR)

Some organisations noted that there is currently no reference to the Data Protection Bill or the impending changes to PECR.

Suggested remedy

The final wording of the Data Protection Bill and revised PECR are not yet agreed, however the Fundraising Regulator proposes to update the Code with references to these as follows:

5.1.1 Data protection is an important issue for all fundraisers. Fundraising organisations **MUST*** comply with all legal requirements relating to data protection. These include:

i) the current Data Protection Act 1998 (*and the* Data Protection Bill 2017 *that will replace this when it becomes enacted in law – this section of the Code will be updated when this happens*);

ii) ii) the Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003, including the requirements of the Telephone Preference Service (*and any revisions to e-privacy legislation that result from the European Commission's review of PECR in 2017 – this section of the Code will be updated when this happens*).

Section 5.1.2: Meaning of "have regard to"

Several respondents advocated:

- that the wording of **5.1.2** needs to be clearer as to how compliance would be judged and assessed in any adjudication. They sought clarification on whether

an organisation would be in breach of the Code if they were to read the latest guidance from the ICO, but then chose to take a different approach which they were confident was legally compliant.

- that reference to GDPR consent guidance should be widened to encompass any GDPR guidance that they release (ie removing the word "consent").
- that the specific reference to the ICO's Fundraising and Regulatory Compliance Conference paper should be removed as it is a time-limited discussion paper rather than formal guidance.
- that a reference to how the ICO framed its guidance in relation to the law would be helpful here.

Suggested remedy

The current proposed wording is as follows:

In addition, organisations **MUST** keep up to date with relevant guidance from the Information Commissioner's Office. This includes the ICO's Direct Marketing Guidance, its Fundraising and Regulatory Compliance Conference paper and its GDPR consent guidance.

The Fundraising Regulator proposes to change this to:

5.1.1 In addition, organisations **MUST** ~~have regard to~~ keep up to date with guidance from the Information Commissioner's Office. This includes *the ICO's* Direct Marketing Guidance, ~~, its Fundraising and Regulatory Compliance Conference paper~~ *and its GDPR consent guidance,* which are designed to promote good practice and help organisations fully understand their obligations.

Section 5.2: Definitions of "Personal data" and "Processing"

Some respondents highlighted that the current definitions proposed are based on the Data Protection Act 1998 rather than the GDPR / Data Protection Bill.

Suggested remedy

The current proposed wording is as follows:

Personal information / Personal data means information/data which relate to a living individual who can be identified –
(a) from that information/data, or
(b) from that information/data and other information/data which is in the possession of, or is likely to come into the possession of, the data controller.

Processing
ICO guidance states that: "The definition of processing is very wide and it is difficult to think of anything an organisation might do with data that will not be processing."
Processing, in relation to information or data, means obtaining, recording or holding information or data or carrying out any operation or set of operations on the information or data, including –

(a) organisation, adaptation or alteration of the information or data (*this includes activities such as entering data on a database, wealth screening, data matching and tele-appending*†)
(b) retrieval, consultation or use of the information or data (*this includes buying data from a third party, storing or checking personal information on a database or using personal data to contact individuals for any reason*†)
(c) disclosure of the information or data (*this includes sharing data with other organisations*†)
(d) alignment, combination, blocking, erasure or destruction of the information or data. (*this includes activities such as suppressing or deleting a donor's details on a database*†)

†Please note that the examples in italics are provided by the Fundraising Regulator for illustrative purposes.

Subject to the current Data Protection Bill passing into law, the Fundraising Regulator proposes to change the wording to align with this as follows:

Personal information / Personal data means information/data which relates to a living individual who can be identified, directly or indirectly, in particular by reference to—
(a) an identifier such as a name, an identification number, location data or an online identifier, or
(b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Processing
ICO guidance states that: "The definition of processing is very wide and it is difficult to think of anything an organisation might do with data that will not be processing."

"Processing", in relation to personal data, means an operation or set of operations which is performed on personal data, or on sets of personal data, such as—

(a) collection, recording, organisation, structuring or storage (*this includes buying data from a third party, storing or checking personal information on a database*)
(b) adaptation or alteration (*this includes activities such as updating personal details)*
(c) retrieval, consultation or use (*this includes activities such as wealth screening or using personal data to contact individuals for any reason*)
(d) disclosure by transmission, dissemination or otherwise making available (*this includes activities such as sharing or publishing data)*
(e) alignment or combination (*this includes activities such as data matching and tele-appending*)
(f) restriction, erasure or destruction (*this includes activities such as suppressing or deleting a donor's details on a database*)

Section 5.2.1: Status of ICO registration / notification

A high number of responses noted that although the ICO will retain the ability to require UK data controllers to undertake some form of annual payment, it is unclear whether this will continue to be termed "notification" and it is not a requirement of GDPR. They suggested that this be reviewed and worded in a way that once the UK Data Protection Bill is implemented, the Code does not require further changes.

The ICO further suggested that this section links to their website (www.ico.org.uk) rather than a specific web page to avoid the possibility of the page going out of date.

Suggested remedy

The current proposed wording is as follows:

Fundraising organisations that process personal information **MUST*** register with the Information Commissioner's Office (ICO) unless they are exempt. Further information on who is required to register and the registration process can be found at https://ico.org.uk/for-organisations/register/.

The Fundraising Regulator proposes to change this to:

Fundraising organisations that process personal information **MUST*** ~~register with the Information Commissioner's Office (ICO) unless they are exempt~~ adhere to any notification or registration as required by the Information Commissioner's Office. Further information can be found at ~~https://ico.org.uk/for-organisations/register/~~ https://ico.org.uk/.

Section 5.2.2: Consistency with ICO wording

- Some respondents noted that **5.2.2(c)** as currently written differs from what is included in ICO guidance (https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/). They suggested that the wording here should be reviewed to align with the ICO as much as possible to ensure meanings and emphasis are consistent.
- It was noted that **5.2.2 b)** introduces a new phrase that is not used in the legislation - "unjustified adverse effects". Some respondents asked if this could either be defined, or rephrased using GDPR terminology.

Suggested remedy
The current draft as proposed states:

5.2.2 When processing personal data (including publically available personal data) for any purpose, organisations **MUST*:**

b) not use the personal data in ways that have unjustified adverse effects on the individuals concerned;

c) give individuals clear and accessible information about how they will process their personal data, including who the organisation is; what they are going to do with the individual's personal information; and (where relevant) who it will be shared with. (*Further information on communicating privacy information to individuals can be found in the ICO's Privacy Notice Code of Practice*).

The Fundraising Regulator proposes to change this to:

5.2.2 When processing personal data (including publically available personal data) for any purpose, organisations **MUST***:

~~b) not use the personal data in ways that have unjustified adverse effects on the individuals concerned;~~

c) give individuals concise, transparent, intelligible and easily accessible information about how they process their personal data. (A detailed list of what **MUST*** be included in privacy information to individuals can be found at https//:ico.org.uk. Further information on communicating privacy information to individuals can be found in the ICO's Privacy Notice Code of Practice).

Section 5.2.5: Legal accuracy

The ICO highlighted that 5.2.5 (b) should refer to the suppression of direct marketing to individuals rather than the suppression of those individuals.

Some organisations also suggested that the phrase "all reasonable steps" would provide a clearer and more accurate summation of what was required of organisations in relation to personal data here than "all necessary steps". The Fundraising Regulator notes that the wording of GDPR specifically refers to ensuring databases are up-to-date "where necessary" and therefore proposes to update the wording to reflect this.

Suggested remedy

The current proposed wording is as follows:

5.2.5 Organisations **MUST** be able to show that all necessary steps have been taken to ensure that:
a) databases are accurate and up-to-date
b) individuals who have asked not to receive direct marketing material are suppressed

The Fundraising Regulator proposes to change this to:

5.2.5 Organisations **MUST*** be able to show that all reasonable ~~necessary~~ steps have been taken to ensure that:
a) databases are accurate and where necessary, up-to-date
b) direct marketing to individuals is suppressed where the individual has asked not to receive it.

Section 5.2.6: Requirement to keep a 'suppression list'

Some organisations suggest that the word "collected" is replaced with the word "processed" within Section 5.2.6, so that the Code is aligned with the terminology used within data protection legislation.

Suggested remedy

The current proposed wording is as follows:

5.2.6 Personal data **MUST*** only be kept as long as necessary to fulfil the purpose for which it was collected.

The Fundraising Regulator proposes to change this to:

5.2.6 Personal data **MUST*** only be kept as long as necessary to fulfil the purpose for which it was ~~collected~~ processed.

Section 5.2.7: Requirement to keep a 'suppression list'

Some respondents pointed out that there are alternative ways of suppressing details beyond producing a "suppression list" For example, they may decide that it is no longer necessary to retain that data, or flag it on their database to ensure they don't send direct marketing to that individual. It was therefore suggest that the Code is amended so that it does not make it a requirement to keep and maintain a 'suppression list', but instead makes it clear that Organisations MUST ensure that it has appropriate systems or procedures in place so that it does not send any direct marketing to individuals who have asked not to receive it.

Some also suggested a further addition to make it clear that individuals can give preferences to not receive marketing through specific channels and therefore the 'suppressions' can be channel specific rather than a blanket 'do not contact' that covers all channels.

Suggested remedy
The current proposed wording is as follows:

5.2.7 Organisations **MUST** maintain a 'suppression list' (containing details of individuals who have asked not to receive direct marketing material) and always check this against lists for direct marketing to ensure they are not contacted (*see also Section 5.7 – "Requests to Cease Direct Marketing"*).

The Fundraising Regulator proposes to change this to:

5.2.7 Organisations **MUST** have appropriate systems or procedures in place (such as a suppression list) to ensure that they do not send any direct marketing to individuals who have asked not to receive it, whether through individual

communication channels or across all channels (*see also Section 5.7 – "Requests to Cease Direct Marketing"*).

Section 5.2.8: data rights of individuals

Several respondents commented that:

- This section is repeated as Section 5.6 and the two should therefore be combined.
- The ICO emphasised that there are two separate rights to be considered when holding an individual's data: the subject access right (Article 15) and the data portability right (Article 20). These should both be reflected in the Code.

Suggested remedy

The current proposed wording is as follows:

5.2.8 Where an organisation holds an individual's personal data to fulfil a contract or because they have gained their consent, the data **MUST*** be provided to that individual if they request it. The data **MUST*** be provided free of charge and in a structured, commonly used format which is openly accessible to software (such as a CSV file).

The Fundraising Regulator proposes to move this section to 5.6 and change the wording as follows:

5.6 Requests from individuals to access their personal data

5.6.1 Where an organisation ~~holds~~ processes an individual's personal data by automated means (*ie through the use of computers and computer software*), they **MUST*,** at the request of the individual, provide the individual with the personal data and information on how it is used if it in accordance with the individual's right of access, subject to any exemptions.

Further information for organisations on what data must be provided and how it must be provided under the Right of Access can be found at https://ico.org.uk

5.6.2 Where an organisation holds or uses an individual's personal data to fulfil a contract or because they have their consent as a lawful basis for processing, the organisation **MUST*** ensure that the personal data can be easily moved, copied or transmitted from one IT environment to another where the individual requests it (whether to the individual's own systems, the systems of trusted third parties or those of new data controllers).

Further information for organisations on requirements under the right to data portability can be found at https://ico.org.uk

Section 5.3.1: Sharing personal data

The ICO suggested that the following wording "and can justify their data sharing through these requirements" should be added to this rule.

Suggested remedy
The Fundraising Regulator proposes to add the ICO's wording as suggested.

Section 5.3.2: Sharing personal data

The ICO highlighted that there may be situations where one organisation will pass the individual's data on to another, and the organisation receiving the data will rely on the individual's consent to hold and use that data. In those circumstances, the organisation receiving the data must be named, and specific consent to that sharing will be necessary.

Some organisations also suggested that it would be useful to add an additional signpost in this section to the ICO's Data Sharing Code of Practice to give further information on the obligations of processing data between organisations.

Suggested remedy
The Fundraising Regulator proposes to add an additional paragraph to section 5.3.2 as follows:

5.3.2 Where personal data is shared between organisations:

- within a federated structure (i.e where one controls the other or where both are under common control), or
- under a data processing arrangement (i.e where one organisation acts on behalf of another organisation under written contract, such as professional fundraisers, data cleansers, or printing houses)

a) the organisational structure / arrangement and the processing purpose **MUST*** be clear enough in the privacy information provided to the individual that the organisation can evidence that processing would fall within the individual's reasonable expectation.
b) Alternatively, where the organisation receiving the data is relying on the individual's consent as the basis to hold and use that data, the organisation receiving the data **MUST*** be named in the consent request, and the specific consent of the individual for their information to be shared **MUST*** be gained by the sender.

(*Further information on data sharing can be found in the ICO's Data Sharing Code of Practice*).

Section 5.3.3: Buying and Sharing Personal data

The ICO highlighted that the requirement for consent to be "unambiguous" may also be found in the Data Protection Directive. The new code rule as it is worded ("from May 2018") suggests that under the Data Protection Act 1998 an ambiguous consent would be acceptable when it is not.

Suggested remedy

The Fundraising Regulator proposes to remove the clause "(from May 2018)" from 5.3.3. The revised wording would read:

Beyond the specific exceptions set out in rule 5.3.2, Organisations **MUST NOT*** share the personal data of an individual with any other organisation for that organisation's marketing purposes without the freely given, specific, informed and ~~(from May 2018)~~ unambiguous consent of that individual to the sharing of the personal data with that other organisation.

Section 5.4: Case Studies

Some respondents suggested that being able to prove that a case study is representative (5.4.3) does not seem to relate to data protection requirements and instead is about good practice in how case studies are sourced, relationships with those portrayed/part of case studies, and how accurate they are. They suggested that this sections might be more aligned with the standards contained in the new section 6 'Content of Fundraising Communications'.

Other responses commented that the inclusion of "*…where practical*" in 5.4.2 ("fundraising organisations **MUST** obtain permission for case studies where practical") was unhelpful and unclear– i.e. it is not clear whether there are any circumstances where you would *not* get permission to use someone's personal information in a case study.

Suggested remedy

The Fundraising Regulator proposes to:

- Relocate section 5.4.3 to section 6.10 as suggested.
- Delete section 5.4.2 on the basis that all personal data processed for the purpose of publication within a case study will be required to comply with data protection law.
- Amend the wording of section 5.4.1 to emphasise that all personal data processed for the purpose of publication within a case study will be required to comply with data protection law. The current wording is as follows:

5.4.1 If using real life case studies, fundraising organisations MUST* comply with the law regarding the processing of personal data (see section 5.and **MUST NOT*** disclose information received in circumstances where a legal duty to keep the information confidential arises.

The Fundraising Regulator proposes to change this to:

5.4.1 If an organisation intends to use a real life example of an individual in a case study, the organisation **MUST*** only process that individual's personal data in accordance with the law (*see **sections 5.1-5.2** above regarding processing personal data lawfully*). Organisations **MUST NOT*** disclose information received in circumstances where a legal duty to keep the information confidential arises, unless there is an overriding legal imperative to do so (for example, a police investigation).

Section 5.5.1: Lawful basis for direct marketing

Several respondents commented that:

- the current wording does not indicate that this is a legal requirement as it is presented as **MUST** rather than **MUST***. They recommend that this is reviewed to provide clarity.
- To further add clarity and make a connection with the subsequent standards, that the wording should refer to consent and legitimate interest as explicit examples, ie: "Fundraising organisations **MUST*** have an appropriate lawful basis (such as 'consent' or 'legitimate interest') for sending direct marketing communications to individuals."
- The ICO suggest that it be clarified here that PECR will restrict sending marketing by electronic means, such as telephone calls, emails, and SMS messages and for several types of communication, such as text messages, emails, and automated telephone calls, consent will nearly always be needed (unless, as some organisations pointed out, they can satisfy the 'soft opt-in' condition for the marketing of products/services). It would be helpful if the Code was clearer about the requirements of PECR in relation to GDPR, as the interface between the two is an issue that is often misunderstood.
- it would be useful to include the 'appropriate' lawful basis above, and make clear in the introductory section (5.5) that for electronic communications, consent will nearly always be needed (unless they can satisfy the 'soft opt-in' condition for the marketing of products/services). While legitimate interest does refer to post/phone in 5.5.6, we think that the importance of understanding the conditions for channels is important enough to be more prominent so as to aid understanding.

Suggested remedy

On the second bullet point above, the Fundraising Regulator considers that the current wording is sufficiently clear, emphasising consent and legitimate interest as the "two most common bases for sending direct marketing communications" and highlighting that "more information on the bases for processing (the "Lawfulness for processing conditions") can be found on the ICO website".

However we propose to:
- add an asterisk to this rule indicate that the rule is a legal imperative.
- add an additional line in the introduction to clarify that there is additional guidance on the lawful bases for each communication channel (live calls, automated calls, text, email, post) on page 24 of the Fundraising Regulator's guidance "Personal Information and Fundraising".
- add an additional line in the introduction to the section to more clearly highlight the distinction for electronic communications as follows:

Alongside data protection regulations that apply to direct marketing, the **Privacy and Electronic Communications Regulations *(PECR)*** *will apply when sending marketing by electronic means, such as emails, text messages and recorded*

telephone calls. In these cases, consent will always be needed as a condition for processing when marketing to individuals, unless the organisation can satisfy:

- *the 'soft opt-in' condition enabling sellers to market similar products/services after an initial purchase (this exception will only be possible in the case of a commercial transaction); or*
- *the exception for marketing to corporate subscribers.*

More information on these PECR exceptions can be found at https://ico.org.uk/ and in the ICO's page on electronic mail marketing.

Section 5.5.3-4: Consent as a basis for direct marketing

Several respondents commented that:

- The proposals in the Code at 5.5.3 a-e) do not quite reflect the GDPR requirement for consent as being a "freely given, specific, informed and unambiguous indication of the individual's wishes". They advocated that there also needs to be recognition that consent is provided through 'clear affirmative action'. One way of doing this is through 'active opt-in methods', but it could also be given through the action of an individual or given verbally. By focusing on 'opt-in' methods in the Code it could give the impression that consent can only be given in writing or a tick box.
- Respondents sought further clarity on what is meant by 'wherever appropriate' in 5.5.3 b, and also on how granular the consent needed to be for the 'different types of processing'.
- Respondents recommended that the use of a 'layered approach' should be referenced in the Code. This is outlined in the text of the ICO's draft consent guidance which states that: "You will need to give some thought to how best to tailor your consent requests and methods to ensure clear and comprehensive information without confusing people or disrupting the user experience – for example, by developing user-friendly layered information and just-in-time consents."
- Clarification was sought on 5.5.3 c) about naming third parties. 5.5.3 refers to consent of the individual to the 'sharing of the personal data with that organisation or other specified types of organisation'. However, 5.5.3 c) "seems to indicate that the third parties need to be named, rather than 'types' of organisation. We believe this should be reviewed and a consistent approach adopted".
- Some respondents queried the use of the word 'emphasise' in 5.5.3 e, noting that GDPR only requires that people are 'informed' about the existence of the right to withdraw consent at any time. It was also pointed out that the wording "*and offer them easy ways to withdraw consent in subsequent communications*" here was duplicated in 5.5.4 a and could therefore be deleted from this section.
- In 5.5.4 b, some organisations suggested that the phrase "or at regular intervals as determined by the organisation" be added to the end of b). As it currently stands, the wording suggests refresh is only required when there is a change.

Suggested remedy

The current proposed wording is as follows:

5.5.3 From 25 May 2018: Where an individual's consent is sought, the consent request **MUST***:
a) use active opt-in methods, such as unticked opt-in boxes.
b) give granular options to consent separately to different types of processing wherever appropriate.
c) be separate from other terms and conditions and not be a precondition of signing up to a service (unless necessary for that service).
d) name the organisation and any third parties who will be relying on the consent.
e) emphasise the individual's right to remove consent at any time and offer them easy ways to withdraw consent in subsequent communications.

5.5.4 From 25 May 2018: If consent has been obtained for direct marketing communications, organisations **MUST*:**
a) offer them easy ways to withdraw consent in subsequent communications.
b) keep consent under review and refresh it if anything changes.

Following consultation with the ICO, we propose to add the following wording as follows:

5.5.3 From 25 May 2018: Where an organisation uses, or intends to use the consent condition as a legal basis for direct marketing communications, the consent obtained **MUST*** be a "freely given, specific, informed and unambiguous indication of the individual's wishes". The Consent **MUST***:

a) be given through a clear affirmative action from the individual to signify consent (for example, using active opt-in methods, such as unticked opt-in boxes or requiring a verbal "yes" response to a question).
b) where the organisation intends to process the individual's data for multiple purposes, give granular options to consent separately to different types of processing (see section A2 of the Fundraising Regulator's guide "Personal Information and Fundraising" for guidance on how to identify whether separate purposes exist for processing personal data or if these purposes can be combined).
c) be separate from other terms and conditions and not be a precondition of signing up to a service (unless necessary for that service).
d) name the organisation and any third parties which will be relying on the consent.
e) inform individuals about their right to remove consent at any time ~~and offer them easy ways to withdraw consent in subsequent communications~~.
f) be recorded in a format which enables the organisation to evidence who consented, when they consented, how they consented, and what they were told.

(With the addition of 5.5.3f we propose to delete section 5.5.2 of the consultation document "Organisations must be able to evidence who consented, how they consented and what they were told" as this covers the same point about the importance of recording consent).

5.5.4 Electronic consent requests **MUST*** be clear, concise and not unnecessarily disrupt the use of the service for which they are provided (such a requirement might be achieved, for example, by breaking a longer privacy notice into shorter pieces of

privacy information to pop up only at the point where personal data is inputted by the individual).

See the ICO's draft GDPR Consent Guidance for further details on obtaining, recording and managing consent.

5.5.5 If consent has been obtained for direct marketing communications, organisations

a) **MUST*** offer the individual in subsequent communications an easy ways to withdraw consent (such as an "unsubscribe" button).
b) **MUST**, at regular intervals as reasonably determined by the organisation, remind the individual of their contact preferences and offer them an easy way to change these preferences if they wish to (such as an "update your communication preferences" button).
c) **MUST*** ensure the individual's record is updated as necessary to reflect changes to their consent or contact preferences.

5.5.6 Legitimate interest as a basis for direct marketing

Comments received regarding this section, included:

- The a-c) requirements for 'evidence' were seen to differ from the ICO guidance in its conference paper of January 2017.
- The specific wording of GDPR at Article 6(1)(f) is processing shall be lawful if 'processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.' There does not seem to be anything in the legislation of ICO guidance that talks about a communication being 'fair and proportionate' in relation to legitimate interest and that a charity can 'evidence' this.
- The potential for confusion with the inclusion of 'necessary' as set out in 5.5.6 a). While it was understand to mean that it is 'necessary to process the data' it could also be read as 'it is necessary for us to use legitimate interest' (as opposed to another legal basis).
- Some organisations saw 5.5.6 b) as confusing and ambiguous and advocated that this was reviewed or, if not part of the legal test for legitimate interest, removed.

Suggested remedy

As indicated in the consultation, the proposed wording on legitimate interest takes into account both GDPR legal wording, ICO guidance on that wording and the findings of the NCVO's working group on donor communications from September 2016 (which recommended in the interest of donors a number of professional standards relating to legitimate Interest which went beyond what the law requires).

The current proposed wording is as follows:

5.5.6 Where an organisation uses or intends to use the Legitimate Interest condition as a legal basis for direct marketing communications by phone or post, the organisation **MUST*** be able to evidence:
a) that it is necessary to use this condition as a basis for communicating.
b) that the communication is legal, fair and proportionate.
c) that any interest which the organisation may have in contacting the individual is balanced against the individual's own interests and rights regarding how their personal data is used.

5.5.7 When sending direct marketing to individuals on grounds of a legitimate interest, organisations **MUST*** explain how their contact data was obtained, and what their legitimate interest is (ie why the charity thinks that the individual might be interested in its cause or its work).

5.5.8 When sending direct marketing to individuals on grounds of a legitimate interest, organisations MUST offer a clear and simple way for the individual to express his or her wish to not be contacted again.

Following consultation with the ICO, we propose to revise the wording as follows:

5.5.6 Where an organisation relies on the Legitimate Interest condition to process data for the purpose of direct marketing by live phone call or by post, the organisation **MUST*** be able to evidence:

a) ~~that it is necessary to use this condition as a basis for communicating.~~ that it has identified a legitimate interest (*ICO guidance notes that this may be an organisation's own interest or the interest of third parties and may include commercial interests, individual interests and broader societal benefits*)

b) ~~that the communication is legal, fair and proportionate.~~that the processing is necessary to achieve that interest (*ICO guidance notes that if the same result can reasonably be achieved in another, less intrusive way, legitimate interests will not apply*)
c) ~~that any interest which the organisation may have in contacting the individual is balanced against the individual's own interests and rights regarding how their personal data is used~~. that it has balanced its interest in processing the personal data against the interests, rights and freedoms of the individual to ensure that the organisation's interests are not overridden by those of the individual (*ICO guidance notes that if the individual would not reasonably expect the processing or it would cause unjustified harm, their interests are likely to override those of the organisation*)
d) the record of decision making, and make this available on request.

~~5.5.7 When sending Direct Marketing to individuals on grounds of a legitimate interest, organisations MUST* explain how their contact data was obtained, and what their legitimate interest is (ie why the charity thinks that the individual might be interested in its cause or its work).~~

5.5.7 When collecting personal information and seeking to rely on the legitimate interest condition to send direct marketing to individuals, organisations:
a) **MUST*** explain what the individual's personal information will be used for.

b) **MUST*** explain the legitimate interests pursued by the organisation.
c) **MUST** offer, in this communication and subsequently in any direct marketing communication sent, a clear and simple means for the individual to indicate that they do not wish to receive direct marketing in future.

~~5.5.8 When sending Direct Marketing to individuals on grounds of a legitimate interest, organisations **MUST** offer a clear and simple way for the individual to express his or her wish to not be contacted.~~

5.6 Requests from individuals to access their personal data

See **section 5.2.8** above.

6.1 Content of Fundraising Communications

A few responders suggested that the phrase "all reasonable steps" was a clearer and more accurate summation of what was required of organisations in relation to communications here than "all necessary steps".

Suggested remedy

The current wording is as follows:

6.1 Organisations **MUST** be able to show that all necessary steps have been taken to ensure that communications are suitable for those targeted.

The Fundraising Regulator proposes to change this to:

6.1 Organisations MUST be able to show that all ~~necessary steps~~ reasonable steps have been taken to ensure that communications are suitable for those targeted.

Section 6.2-6.14

A number of other points were raised in relation to section 6 which did not relate directly to data protection. The Fundraising Regulator proposes to look at these at a future date as part of its wider review of the Code.

7.1.1 Mailing Preference Service

A high proportion of respondents noted that there is a significant change proposed at 7.1.1 on how fundraisers work with the Mailing Preference Service (MPS). They emphasised that this proposal would significantly change what the MPS service was set up to do and mean that unless individuals have provided consent to that charity, no direct marketing mailings can be sent. They highlighted that MPS is specifically set up to stop 'unsolicited' mailing (it is not a statutory service like the TPS) and clearly explains to individuals that if they sign up "You can expect to continue to receive mailings from companies with whom you have done business in the past." This means that as long as organisations can satisfy the legitimate interest ground, a

registration on the MPS would not stop that organisation sending direct marketing by post.

Suggested remedy

The current proposed wording is as follows:

7.1.1 In addition to complying with section 5.7, Organisations **MUST NOT** send direct marketing mailings to individuals registered on the Mailing Preference Service unless the person who registered their address has notified the organisation specifically that they consent to receiving direct marketing mailings from them.

The Fundraising Regulator proposes to change this to:

7.1.1 In addition to complying with section 5.7, Organisations **MUST NOT** send direct marketing mailings to individuals registered on the Mailing Preference Service where no prior relationship can be evidenced. Organisations **MUST** consider MPS registration as part of their Legitimate Interest Assessment if intending to process an individual's data for direct marketing purposes under the legitimate interest condition.

8.2.3: The Telephone Preference Service

ICO suggested that the reference to consent for marketing calls being valid 'for the time being' should be restored as this this phrasing comes from the text of PECR itself. Some organisations also highlighted that contrary to what the proposed code revision implies here, individuals register their telephone number rather than their address.

Suggested remedy

The current proposed wording is as follows:

8.2.3 b) Organisations **MUST NOT*** make direct marketing calls to Telephone Preference Service (TPS)/Corporate TPS (CTPS)- registered numbers unless the person who registered their address has notified the organisation specifically that they consent to receiving direct marketing calls from them.

The Fundraising Regulator proposes to amend this wording as follows:

8.2.3 b) Organisations **MUST NOT*** make direct marketing calls to any number registered with the Telephone Preference Service (TPS) or Corporate Telephone Preference Service (CTPS), unless the person with the registered number has notified the organisation specifically that they consent to receiving direct marketing calls from them for the time being.

8.3.1: Key requirements - Telephone

- The ICO highlight that PECR will apply to this section as it relates to telephone calls being made for marketing purposes. Automated telephone

calls should not be made without the individual's consent, and live telephone calls should not be made to numbers registered with the Telephone Preference Service. If the individual has previously given a clear indication that they do not wish to receive marketing, they should not be contacted.

- In addition, several organisations pointed out that Ofcom's guidance on nuisance calls changed in 2017. 8.3.1k) of the Code should reflect the less prescriptive tone of the new guidance and emphasise that misuse covers a number of practices, including, but not limited to silent calls.

Suggested remedy

The Fundraising Regulator proposes to change this as follows:

8.3.1 Key Requirements

Section 5: Personal information and Fundraising *includes requirements for telephone fundraisers under the General Data Protection Regulation and Privacy and Electronic Communications Regulations. The following rules should be read in conjunction with the requirements highlighted in that section.*

a) Automated telephone calls **MUST NOT*** be made to individuals without their consent.

~~b)If the telephone call is first contact with a donor, the caller **MUST** ask if the recipient consents to being contacted at that time.~~ Calls **MUST NOT** be made after 9pm, unless requested by the recipient.

b) If an individual has previously given a clear indication that they do not wish to receive marketing, they **MUST NOT*** be contacted (see also **Section 5.7 – "Requests to Cease or not begin Direct Marketing**").

c) Organisations **MUST*** identify themselves when making a Direct Marketing call.

d) If the telephone call is first contact with a donor, the caller **MUST** ask if the recipient is happy to be contacted at that time. If the recipient asks not to be called again, the fundraising organisation MUST* comply with the request.

e) Fundraisers **MUST** make clear that the call is seeking financial or other forms of support and **MUST*** make appropriate disclosure statements.

f) If an organisation uses a subcontractor (such as an external telephone fundraiser who falls within the definition of professional fundraiser), then the subcontractor **MUST** inform contacts of the identity of the organisation on whose behalf the calls are being made along with details of the sub-contractor's remuneration in connection with the appeal.

g) In England and Wales, the appropriate statement **MUST*** be made during each call and a written statement must be sent within seven days of any payment being made by the donor to the professional fundraiser.

h) In Scotland, information about remuneration given by a professional fundraiser during a call **MUST*** be available in writing and offered to the donor.

i) Organisations **MUST*** avoid misuse of an Electronic Communications Network or Service to contact donors (including making silent or abandoned calls).

Ofcom's Revised Statement on the Persistent Misuse of an Electronic Communications Network or Service (2016) gives guidance about silent calls and other forms of nuisance call, including what factors it considers in determining whether persistent misuse of an electronic communication network or service has occurred.

The Direct Marketing Association has also provided practical Advice on Persistent Misuse (2017) for contact centres in the light of Ofcom's statement.

j) In addition to the rule outlined in **section 1.2g**, Fundraisers **MUST NOT**, at any point in a telephone call, be unreasonably persistent or place undue pressure on the recipient to donate, and in particular, **MUST NOT** ask for a financial contribution more than three times during that call.

k) If a call recipient asks not to be called again, the fundraising organisation **MUST*** comply with the request (see also **Section 5.7 – "Requests to Cease or not begin Direct Marketing**").

14: Text messages (SMS) and Multimedia messages (MMS)

Some organisations suggested that the ICO has confirmed that a Direct Marketing exception existed for SMS and MMS donations and that this should be reflected in the Code. On the initial confirmation message that donors receive having made an SMS or MMS donation, it was reported that the ICO has said it is acceptable for the message to include information on how the individual can give their consent to hear more about the cause/campaign (for example, thank you for your donation of £5 to charity X. If you would like to hear more about our work and ways you can support us, reply 'YES' to this message'.

Suggested remedy

Following consultation with the ICO, the Fundraising Regulator does not propose to include this as an exception in the Code at present. There is no specific exception within GDPR or PECR for SMS or MMS messages and marketing.

15.3.2: Participants/attendees

One respondent (IoF) said that 15.3.2 e) did not relate to data protection but to 'permissions' or consent for other terms and conditions (e.g, health and safety). They asked the Fundraising Regulator to confirm this, and if so, ensure that the reference to Section 5 is clear and appropriate.

Suggested remedy

The current proposed wording is as follows:

15.3.2 e) Any consents legally required for the participant to be involved in an event **MUST*** be obtained in writing in advance of the event taking place.

Section 5: Personal information and Fundraising includes further information on requirements relating to data protection.

The Fundraising Regulator proposes to change this to:

e) Any consents legally required for the participant to be involved in an event (including, where relevant, consent to accept legal terms and conditions, ensure health and safety and protect personal data) **MUST*** be obtained in writing in advance of the event taking place.

Section 5: Personal information and Fundraising includes further information on requirements relating to data protection.