Amnesty International United Kingdom Section
Amnesty International (UK Section) Charitable Trust
Amnesty Freestyle Limited

Data Protection Policy

Final Draft: 20 January 2011 by BWB

Updated: 23rd July 2015 by Craig Humphries – Head of Finance & Data Analysis - AIUK

Bates Wells & Braithwaite London LLP
2-6 Cannon Street
London EC4M 6YH

Tel: 020 7551 7777
Ref: MOR/010923/0054

Index

1. Introduction

1.1 Amnesty International UK (**"Amnesty"**) (which includes Amnesty International United Kingdom Section (**"UK Section"**) and Amnesty International (UK Section) Charitable Trust (**"UK Trust"**) and Amnesty Freestyle Limited ("Freestyle") is committed to complying with privacy and data protection laws including the Data Protection Act 1998 (**"the DPA"**). Amnesty regards its database as a hugely valuable asset that it depends on for its fundraising and campaigning force. This data protection policy (**"the Policy"**) sets out the principles which we will apply when handling individuals' personal information.

1.2 It is the responsibility of all employees and volunteers who deal with personal information to ensure Amnesty complies with this Policy. Employees and volunteers should apply the guidance in this document whenever they are dealing with personal information.

1.3 A failure to comply with this Policy could expose Amnesty to enforcement action by the Information Commissioner's Office (**"the ICO"**). The ICO has powers to issue notices requiring compliance with the DPA, to require organisations to co-operate with its enquiries, to search and seize material and to issue substantial fines. This could ultimately result in restrictions being imposed on our use of some or all of our databases or in complaints or claims for compensation from affected individuals. There is also a risk of very damaging negative publicity for Amnesty if any breach is made public.

1.4 For these reasons, it is important that all employees and (where appropriate) volunteers familiarise themselves with this Policy and attend all training sessions in respect of the care and handling of personal information. Failure to comply with this Policy could amount to misconduct, which is a disciplinary matter. Serious breaches could also result in personal criminal liability.

1.5 This Policy may be amended from time to time to reflect any changes in legislation or internal policy decisions.

2. Status of this Policy

This Policy does not form part of the formal contract of employment for staff. However, it is a condition of employment that employees will abide by the rules and policies made by Amnesty from time to time and that includes this Policy.

3. Policy definitions

The following terms are used in this policy:

Term		Meaning
3.1	**"Amnesty Groups"**	includes Amnesty Student Groups, Amnesty Local Groups and Amnesty Youth Groups.
3.2	**data subjects"**	include all living individuals about whom Amnesty holds or handles personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
3.3	**"Electronic Communications Regulations"**	means the Privacy and Electronic Communications (EC Directive) Regulations 2003. These contain laws that add to the DPA including laws about e-marketing.

3.4	**"European Economic Area"**	includes all countries in the European Union as well as Norway, Iceland and Liechtenstein.
3.5	**"personal data"**	means data relating to a living individual who can be identified from that data (or from that data and other information in possession of Amnesty), in particular information with the data subject as its focus which may affect the individual's privacy in some way.
3.6	**"data controller"**	is the entity which determines the purposes and the manner in which personal data is used. It must comply with the DPA. UK Section and UK Trust are both data controllers.
3.7	**"data processors"**	any person company or other organisation which processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it will include suppliers which handle personal data on Amnesty's behalf such as outsourced web hosting providers, fulfilment houses and professional fundraisers.
3.8	**"ICO"**	means the Information Commissioner's Office (the authority which regulates personal data in the UK).
3.9	**"processing"**	is any activity that involves use of the data. It includes obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
3.10	**"sensitive personal data"**	is information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. It does not include financial information, or information about an individual's age. Sensitive personal data can only be processed if one of a limited number of strict conditions apply. One of these is a condition requiring the express consent of the person concerned.

4. Data protection principles and staff responsibilities

The Data Protection Principles

4.1 The DPA is concerned with "the rights and freedoms of individuals with regard to the processing of personal data".

4.2 Amnesty will comply with the following principles in respect of any personal data which it deals with as a data controller.

Personal data shall be:

4.2.1 obtained fairly and lawfully;

4.2.2 processed for the purposes which have been specified, and not in any way incompatible with those purposes;

4.2.3 adequate, relevant and not excessive for the purposes;

4.2.4 accurate and, where necessary, kept up to date;

4.2.5 not kept for longer than purposes require;

4.2.6 processed in accordance with the rights of data subjects;

4.2.7 kept secure;

4.2.8 transferred to countries outside the European Economic Area (see definitions) only with adequate safeguards.

5. Staff responsibilities

The Data Protection Compliance Officer

5.1 Amnesty's Data Protection Compliance Officer is responsible for ensuring compliance with the DPA and with this Policy. The Data Protection Compliance Officer is the Head of Finance & Data Analysis. Any questions or concerns about the interpretation or operation of this policy should be referred to him or her, in the first instance.

Other employees

5.2 All employees and volunteers (where they will be processing personal data for Amnesty) should be aware of their basic responsibilities under the data protection legislation. If you are in any doubt, or if you think that this Policy has not been followed in respect of personal data about you or anyone else, you should seek clarification on any issues from the Data Protection Compliance Officer immediately.

6. Capturing and handling the personal data of supporters and others

6.1 In order to achieve the crucial balance between adhering to regulation and making full use of our data in as unrestricted a manner as possible, we need to maximise the opportunities for supporters to clearly express their preferences with a full understanding of the implications of their choices while minimising the assumptions we make that would restrict our ability to communicate with them.

Define a clear, specific purpose for the data

6.2 The first two data protection principles (listed in section 4 of this Policy) require that data is obtained fairly and lawfully and processed for purposes communicated to the data subject.

6.3 To do this, every time Amnesty receives personal data, which it intends to keep (e.g. supporter or activist data), it must give the subjects of that data **"the fair processing information"**. In other words:

6.3.1 who will be holding it, i.e. UK Section or UK Trust, or both; and

6.3.2 why Amnesty is collecting it and what we intend to do with it; and

6.3.3 anything else necessary to make sure Amnesty is using their information fairly, for example – if you plan to pass your marketing lists to other organisations.

6.4 In most cases, Amnesty's primary purposes in capturing personal data is to keep our supporters and other interested parties informed, promote campaigning, activism and education and to carry out fundraising activities to support this work.

6.5 This fair processing information can be provided on web pages, or in mailings or on donation forms.

6.6 Most commonly, when capturing data we will include the general permissive statement set out in the Model Statements document at Appendix E. This allows us to use data for a wide set of purposes.

6.7 Please refer to the Data Protection Compliance Officer if capturing data without using the Model Statements or if you are unsure how to deal with personal information which has been captured.

Apply the same rules when capturing information by telephone

6.8 When speaking to someone on the telephone, we still need to make clear what we will use their personal data for.

6.9 If during a phone call, we capture a name and address to send out information we should inform the individual that Amnesty would like to use their information to send them further information or communications in future. This is part of the "fair processing information".

What to record when capturing information

6.10 Keeping track of the reason given when personal data has been captured enables us to justify how we use it if challenged. Also, going forward, it is important to understand what explanation was given to a supporter when his or her information was collected. A record of what statement was used when collecting a person's data should be recorded or if not the wording of the statement itself at least the preferences expressed by the data subject, e.g. campaign mailings only.

6.11 Under the Electronic Communications Regulations, we **must** be able to show consent for use of email addresses for marketing, if challenged, and when it was obtained.

Sensitive personal data

6.12 On some occasions Amnesty collects other information about supporters in addition to contact details. Information about a person's ethnicity or political beliefs for instance is not essential for the purpose of making a donation or sending someone marketing updates. This extra information may help us understand what kind of people want to support us and therefore improve our direct marketing efforts, or may enable us to target campaigning. We can collect and use data for this purpose, so long as we explain why and, if data is "sensitive", obtain explicit consent or comply with one of the other conditions referred to in section 6.1.3 below.

6.13 "Sensitive" personal data is defined in section 3.10. Sensitive personal data can only be processed in limited situations. The most relevant ones are when:

6.13.1 The individual has given explicit consent to the processing;

6.13.2 The processing is necessary so that Amnesty can comply with employment law;

6.13.3 The processing is necessary to protect the vital interests (i.e. a matter of life or death) of:

(a) the individual (in a case where the individual's consent cannot be given or reasonably obtained), or

(b) another person (in a case where the individual's consent has been unreasonably withheld),

6.13.4 The processing is carried out by a not-for-profit organisation which exists for political, philosophical or trade-union purposes and does not involve disclosing personal data to a third party, unless the individual consents. The processing must be carried out with appropriate safeguards in place for the rights of the data subject and should relate only to individuals who are either members of the organisation or have regular contact with it in connection with the organisation's purposes (see section 6.15 below);

6.13.5 The individual has deliberately made the information public;

6.13.6 The processing is *necessary* in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights;

6.13.7 The processing is necessary for administering justice, or for exercising statutory or governmental functions;

6.13.8 The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality;

6.13.9 The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

6.13.10 The processing is necessary to prevent or detect crime or protect the public against malpractice or maladministration.

6.14 In most cases Amnesty will be relying on the first condition listed (section 6.13.1) – the explicit consent of the data subject. For advice on how Amnesty can obtain a person's explicit consent to processing sensitive personal data, please see Appendix E.

6.15 The definition of "sensitive personal data" includes a person's political opinions. There is an argument that the fact that an individual is a member of Amnesty could, on its own, constitute

sensitive personal data as it relates to that person's political opinions or beliefs. Amnesty believes that if this was argued, in most cases, it would be able to rely on the exemption set out in section 6.13.4 above and would not need to obtain individuals' explicit consent to process information about their membership or support of Amnesty. If you are unsure whether any personal data you are processing is sensitive and falls within the exemption please speak to the Data Protection Compliance Officer.

Do not make unnecessarily restrictive promises to supporters and other contacts

6.16 It is important to be open and transparent with our supporters about how their information will be used. You should not include overly restrictive promises in data collection statements or privacy policies, e.g. *"we will only use your information for this campaign".*

6.17 This is not a legal requirement and may prevent Amnesty from making optimal use of its activist and donor databases. Try to use wording from the Model Statements or check with the Data Protection Compliance Officer if you are unsure.

6.18 Marketing fields should always give individuals as much choice as possible so that it is possible for an individual to opt-out of receiving communications that are not desired without excluding him or herself from receiving any communications from Amnesty.

Sharing supporter data with other organisations

6.19 From time to time we exchange contact details of supporters with similar organisations who may wish to fundraise from those supporters. We should always make this clear as outlined in the Model Statements.

Email addresses are not shared

6.20 We do not trade email addresses as other organisations cannot send marketing emails unless the supporter in question has specifically requested marketing communications from that organisation (see sections 9.3 and 9.7).

Accurate data

6.21 Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of personal data at regular intervals. Inaccurate data should be corrected and out-of-date data should be archived or destroyed as appropriate (see Appendix B).

7. Photographs and CCTV footage

Photographs

7.1 Clear images of individuals are personal data for the purposes of the DPA since, at least to those who know the individual, it is possible to identify the individual from the image. Photographs of supporters or others collected or held by Amnesty should be treated in the same way as any other personal information.

7.2 Photographs may raise copyright issues. If you are inviting supporters to send photographs to Amnesty for a particular campaign or other purpose, you should first consider how Amnesty wishes to use the photograph. If it wants to publicise it and use it for its own purposes, you should ensure that the individual who has taken the picture has consented to this in advance. You can do this by including simple terms and conditions when inviting people to submit photographs. For appropriate wording for terms and conditions, please speak to the Data Protection Compliance Officer.

7.3 Where you intend to take photographs of members and supporters attending events, you should ask people to sign the consent forms set out in Appendix F or, where this is not possible, put notices up at the event notifying people that they may appear in event publicity. Individuals should be given an opportunity to ask organisers not to publish photographs or create images of them.

7.4 **WARNING: if you are doing anything with photographs of people who are under 18, please ensure that you are also complying with Amnesty's Safeguarding Children and Young People Guidance.**

CCTV footage

7.5 Amnesty operates CCTV cameras for security reasons. The CCTV footage captured on those cameras is also likely to be covered by the DPA. The ICO has prepared a CCTV Code of Practice. The Surveillance Camera Commissioner also published a code of practice on 2nd July 2015 detailing it's 12 guiding principals found here: https://www.gov.uk/government/publications/surveillance-camera-code-of-practice-ownerinstaller-responsibilities. Amnesty has drawn up its own code which is based on that model. This is attached to this Policy as Appendix H.

8. Personal data collected from the public domain

Collecting personal data from the public domain

8.1 From time to time Amnesty collects information on prospective donors and supporters from information which is publicly available, and not from the individuals themselves. Even where information is collected from the public domain, most of the provisions of the DPA will still apply to that information, including the requirement to provide the "fair processing information" (see section 6.3).

8.2 There are mechanisms for complying with the notification requirements. One way to do this is by sending a mailing to all of the individuals whose data Amnesty has obtained from the public domain, informing them about a particular campaign. The mailing can include a short notice informing people that Amnesty is holding their information and, in broad terms, the purposes for which it is so doing. This should not be done without consulting with the Data Protection Compliance Officer. Please note this mechanism can be used for postal mailings only. To send emails containing marketing, the requirements set out in section 9.3 of this policy need to be complied with.

Public domain information and sensitive personal data

8.3 Even if the data gathered from the public domain is sensitive the DPA permits data controllers to process it. This is provided that the personal data has been made public as a result of steps deliberately taken by the data subject. Amnesty may therefore compile or process sensitive personal data (see definitions) relating to individuals provided the information being processed has been made public by the individual him or herself without obtaining an individual's prior consent or satisfying another Schedule 3 condition. Please note that even if a person has put their information in the public domain Amnesty must still provide them with the fair processing information (see section 6.3).

Paper files

8.4 Most paper records (i.e. data not held on a computer system) technically are not covered by the DPA. The only paper records which are subject to the DPA are data which is held in a highly ordered filing system e.g. some HR records. In relation to paper records containing personal information taken from the public domain (or from elsewhere) Amnesty is not technically required to provide

individuals with the fair processing information or to otherwise comply with the DPA in relation to them.

8.5 However, to follow best practice, Amnesty should treat paper records as though the DPA applies to them.

9. Marketing to supporters

Overview of marketing

9.1 "Direct Marketing" is interpreted very widely by the ICO as covering a wide range of activities which will apply not just to the offer of sale of goods or services, but also to the promotion of an organisation's aims and ideals. Therefore, it is not just fundraising. Most communications sent by Amnesty to supporters and activists will include direct marketing and will be caught by the Electronic Communications Regulations.

Postal marketing/Direct mail

9.2 When sending marketing materials by post, you should remember:

9.2.1 In most cases, Amnesty will not need a person's prior consent to send them direct mail.

9.2.2 The DPA gives people a right to ask data controllers such as Amnesty to stop processing data about them for direct marketing purposes. Amnesty should record all such requests on a "suppression list" and refrain from contacting those people (unless they ask Amnesty to start contacting them). **There are no exceptions and Amnesty must comply with requests within a reasonable period of time.** In its guidance, the ICO says that most requests should be complied with within 28 days.

9.2.3 An individual who wishes to prevent personally addressed marketing material being sent to him may register with the Mailing Preference Service ("**MPS**"). You should not send any unsolicited direct mail by post, to a person who has registered with MPS, unless that person has stated that they do not object to receiving such mailings.

Email and SMS marketing

9.3 The following rules apply when sending emails or text messages that contain any type of marketing to personal email addresses.

9.3.1 Amnesty must have consent *before* making any kind of approach by email. This consent must have been given directly by the recipient to Amnesty or its agents (such as professional fundraisers) unless it is given to someone else in the first person, such as in the following form: *"I would like to be kept updated about Amnesty's work and what I may help to achieve"*. Please note that third parties (but not our agents such as fulfilment houses) who have agreed to share supporter data with Amnesty should be asked to use this form of words in their mailings.

9.3.2 When sending emails to groups or lists, one person's email address should never be visible to other recipients (e.g. use the 'bcc' field).

9.3.3 The emails must make it clear in the subject line that the email contains marketing. For instance "Amnesty Appeal for [ ]".

9.3.4 The emails should, as matter of best practice, provide clear instructions for unsubscribing from future emails of that kind (for example, by providing an email address to reply to) though a postal address is acceptable.

9.4 Electronic marketing sent to corporate organisations and public bodies must say who the marketing is from and provide Amnesty's contact details. Consent is not needed in the way that it is for emails to individuals. However, the ICO recommends that electronic mail sent to organisations is treated in the same way as electronic mail sent to individuals. In other words, that data controllers respect an organisation's wish not to receive marketing. However that is a matter of good practice and is not required by law.

9.5 Also, if you are sending emails to an individual at an organisation, that person still has a right under the DPA to ask Amnesty to stop sending him or her marketing (see section 9.2.2).

9.6 These principles apply to unsolicited direct marketing by fax, email and text message as well as by voicemail messages.

Telephone marketing

9.7 You should never make marketing telephone calls to an individual or organisation who has told Amnesty they do not want calls from us or to any numbers on the Telephone Preference Service ("**TPS**") list unless the individual or organisation has stated that they do not object to Amnesty making such calls.

9.8 If Amnesty or an agency working on behalf of Amnesty is making marketing telephone calls, you or the agency must:

9.8.1 stop making telesales calls to their number if a subscriber asks you to;

9.8.2 identify yourself as calling from Amnesty; if using a sub-contractor, the sub-contractor's call centre staff must identify the instigator of the call – i.e. Amnesty;

9.8.3 if asked, provide a valid business address or free phone number at which you can be contacted;

9.8.4 maintain suppression lists to avoid calling people who have opted out of receiving telemarketing calls either by notifying Amnesty directly or by notifying TPS.

9.9 Amnesty can make unsolicited calls to a TPS registered supporter, where that person has notified Amnesty that they do not mind receiving calls on the TPS registered number. However, a supporter can withdraw that consent at any time, in which case Amnesty cannot make further calls to that number.

9.10 Where an individual enlists with TPS after consenting to receive marketing communications from Amnesty, provided the individual has previously given a clear notification that they are happy to receive marketing calls from Amnesty, his or her registration with the TPS should not override the initial consent given to Amnesty.

9.11 However, if a list of numbers is obtained from a third party, even if individuals on the list have consented to receiving unsolicited marketing from charities generally, Amnesty should screen the list against TPS. Individuals can give consent to receiving unsolicited calls which overrides TPS registration, but this is only valid where the overriding consent is given to the organisation in question, i.e. Amnesty. Mobile numbers can also be registered on the TPS. Amnesty can, however, send texts, pictures or video messages without needing to screen against TPS, but prior consent will be needed before sending such messages.

9.12 Where Amnesty buys lists of telephone numbers of supporters in relation to whom it already holds other contact details, Amnesty should screen the numbers on that list against TPS.

Amnesty's identity and contact information

9.13 All marketing materials must provide appropriate contact details so that the individual or organisation receiving the marketing can easily contact Amnesty.

10. Viral marketing

Video Clips

10.1 Amnesty can ask supporters to send campaign video clips to their friends and include a statement inviting recipients to sign up to receiving Amnesty communications. Providing that statement complies with this Policy and Amnesty only receives and uses recipients' contact details where they have voluntarily consented to this, this practice should not cause any compliance issues for Amnesty.

"Tell a friend"

10.2 This is where individuals are invited to tell friends about Amnesty by:

encouraging their friends to contact Amnesty, e.g. by sending them an Amnesty campaign email.

10.3 When using this type of marketing, you should remember that Amnesty can only send emails to new supporters where *they* have consented to receiving email marketing from Amnesty and they have got in touch with Amnesty directly. It is Amnesty's policy not to send marketing to people where it has been given their email address by their friends.

11. Marketing to children

Overview

11.1 There is no age fixed in law at which children are deemed to have capacity to give consent for the purposes of the DPA or the Electronic Communications Regulations.

11.2 It is Amnesty's policy to ensure that all core materials it produces are suitable for people over the age of 14. All core materials should be approved by the Content Approval Panel **("CAP")**. CAP will make decisions on age suitability of materials in consultation with the Education and Student Team **("EST")**.

11.3 Amnesty should also, as a matter of best practice, take steps to demonstrate a strict application of the requirements of DPA and the Electronic Communications Regulations in relation to children.

11.4 **WARNING**: **when you are doing anything with personal data relating to people under 18, please ensure that you are complying with Amnesty's Safeguarding Children and Young People Guidance. Please discuss any need for further information or assistance with the Designated Child Protection Officer and a Deputy Designated Child Protection Officer**

Targeting children online

11.5 For web campaigns specifically targeted at children, Amnesty should seek to use language in privacy policies and other statements which is likely to be understood by the children concerned. It should take into account the fact that children may have a lower level of understanding. You may also wish to include warnings, advising children not to share their information with other online users and to get parental consent before providing any personal information online.

Mailings targeted at children

11.6 In preparing mailings aimed at children, Amnesty should always tailor the contents of those mailings to reflect the risk of those mailings causing shock or distress to children.

Data collection statements for children

11.7 Amnesty must adopt a common sense and good practice approach when collecting and processing children's data. Amnesty's policy is to only contact children who are younger than 14, where

11.7.1 it has the consent of a child's parent or guardian; or

11.7.2 it is collecting information only for the purposes of very limited future contact.

Other contact

11.8 Where Amnesty is sending messages to its wider supporter base and wishes to avoid under 14s seeing mailings, it should consider adding "warning" text to the subject headings of campaign emails which contain particularly upsetting images or text.

11.9 All new contacts should be asked to confirm their age at the point when Amnesty collects their information, e.g. "*So that we can ensure that you receive appropriate* mailings*, if you are under 18, please tell us the year you were born*." This way Amnesty can save this information and use it to avoid sending inappropriate mailings to children. Please see Appendix E for more details.

12. Sharing personal data with data processors

12.1 Amnesty is required to take particular security precautions when it uses third parties to process personal data on its behalf.

12.2 Third parties may include IT contractors, providers of hosting services for Amnesty websites, professional fundraisers, outsourced service providers, payroll providers, fulfilment houses and disaster recovery service providers.

12.3 These third parties are data processors (see definitions page). Staff who are responsible for the selection or appointment of any data processors, or are involved in contract negotiations with data processors must:

12.3.1 select only data processors who provide sufficient guarantees in respect of the technical and organisational security measures they will use in relation to the processing of personal data;

12.3.2 ensure that Amnesty enters into a written contract with each data processor. It is important to do this before the processing actually begins. Please use Amnesty's standard data processing contracts which is annexed at Appendix C;

12.3.3 where the data processor is located outside the European Economic Area, Amnesty will probably need to enter into an EC approved contract. If you think this might be necessary, please speak to the Data Protection Compliance Officer;

12.3.4 if you have already provided a data processor with personal data under a standard contract (or even without any contract) you should ask the provider to sign up to the standard data processing agreement retrospectively;

12.3.5 ensure that each data processing contract makes it clear that data processors must only act on instructions from Amnesty. The law makes Amnesty responsible for the processing of all personal data, even if it is carried out on its behalf by a data processor. It must, therefore, maintain control over such processing at all times.

12.4 Where a member of staff is not sure whether a data processing agreement is needed, please ask the Data Protection Compliance Officer.

13. Data security

13.1 Amnesty must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

13.2 The DPA requires us to put in place procedures and technology to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if the third party agrees to comply with those procedures and policies, or if he puts in place adequate measures himself (see section 12).

13.3 Amnesty has put in place procedures and technology to maintain the security of all personal data from the point of collection to the point of destruction.

13.4 If personal data held is also sensitive, an additional level of security is applied, for instance, if sensitive personal data is held on a memory stick or other portable device you should always encrypt it because the potential reputational and other damage to Amnesty will be greater if the information is lost or stolen. When deciding what level of security is needed, your starting point should be to look at whether the information is sensitive or highly confidential and how much damage could be caused if it fell into the wrong hands.

13.5 The following security procedures must be followed in relation to all personal data.

13.5.1 **Entry controls:** Any stranger seen in entry-controlled areas should be reported.

13.5.2 **Equipment:** Staff should ensure that individual monitors do not show confidential information to individuals who are not employees of Amnesty and that they log off from their PC when it is left unattended.

13.5.3 **Secure lockable desks and cupboards:** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal data is always considered confidential.)

13.5.4 **Methods of disposal:** Paper documents should be shredded or recycled. Where personal data is recycled, only reputable companies who have given appropriate security undertakings should be used. Memory sticks and CD-ROMs and other media on which personal data is shared should be physically destroyed when they are no longer required.

13.5.5 **User access controls:** All staff should share their password only on a need to know basis and should be an exception rather than the rule. Passwords should be changed on a regular basis; computers should have password activated screen savers that can be turned on whenever the user is away from his or her desk; passwords should be of a 'complex' nature that include a mixture of letters and numbers and ideally special characters; avoid passwords that are easy to guess such as an employee's name or date of birth; different rights of access to all our systems and software should be allocated to different users depending on job description and need to access personal or confidential data. If a requirement exists for a third party supplier to access Amnesty's systems and data then they must be provided with a unique login and password and never a staff or volunteers login details. All third party suppliers accessing our systems MUST also have signed and agreed to accept Amnesty's data protection and confidentiality requirements. It is the responsibility of the staff member or volunteer managing the supplier relationship to ensure this is strictly adhered to. The Data Protection Compliance Officer and Amnesty's IT Team should be consulted immediately if concerns arise around any issue of User Access Controls.

13.5.6 **Backing up data:** Daily back ups are taken of all data on Amnesty's systems; staff and volunteers should not be storing data on local drives or removable media as these will not be backed;

13.5.7 **Disaster recovery**: copies of personal data are stored off site in a secure and fire-proof location; a business continuity plan has been implemented and will be followed in the event of a disaster; disaster recovery and business continuity plans are tested periodically. Uninterruptible power supplies are in place for key systems.

13.5.8 **Data retention policy:** Amnesty advocates a policy of deleting data that is no longer current. If you have data that you know is no longer required, you should destroy it.

See Appendix B for details of when different types of data should be destroyed. Data should be destroyed in accordance with section 13.5.4.

13.5.9 **Travelling with personal data:** Staff must keep data secure when travelling or using it outside of Amnesty's offices. For instance, documents and laptops must be kept secure (not left lying around off site). Amnesty is working towards implementing a system under which personal data stored on laptops, blackberries and other portable media is encrypted, using effective and up to date encryption software. Where you are using media that contains suitable software, you must make arrange for encryption to be enabled. To arrange for a device to be encrypted please contact the IT team before using.

Data stored on computers when working at home must be password protected, and kept confidential. Up to date security scanning software (anti virus, anti malware) must also be installed on all computers being used to access the Amnesty Citrix Portal and systems.

When you are working from home, you should ensure that the laptop or computer you are using is securely protected from theft while you are away from it (speak to the Head of Facilities and IT for more details).

13.5.10 **Reporting & analysis:** Reports should be anonymous whenever possible – i.e. where personal details like names and addresses are not required, they should not be included.

13.5.11 **Secure exchange of data:** Data must always be transferred in a secure manner. The degree of security required will depend on the nature of the data; the more sensitive and confidential the data, the more stringent the security measures should be. The following precautions should be considered:

(a) Use registered post or courier. Never send a CD/DVD or memory card/stick with lots of personal data by normal post. Any item sent via registered post or courier must always be encrypted and password protected.

(b) Use password protection (on files) if sending by email – but recognise this is not very secure and should only be used for non-personally identifiable and non-sensitive information. Excel and Word passwords are not a strong enough solution if you wish to share a document containing sensitive information and such information must always be sent with encryption and a strong password. Contact IT helpdesk if you require assistance.

(c) Never send financially sensitive or other sensitive data by email unless encrypted. Contact IT helpdesk if you require assistance.

13.6 IT Asset Disposal is an important aspect of adhering to Data Security principals and Amnesty will ensure that all assets that risk compromising data security will be disposed of in a manner that ensure that any data that may have been stored on the IT asset will not be recoverable in any way. This may be through either an appropriately ISO accredited third party supplier either undertaking recycling or destruction of the IT asset or using the in-house IT team applying appropriately thorough methods of destruction of the IT asset. The Head of Facilities and IT will be responsible for ensuring Amnesty adhered to the ICO guidance around IT asset disposal for organisations. https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

13.7 Cloud Computing services and data storage is an increasing methodology used and uptake and availability of Cloud based services will continue to grow. It is important that oversight and assurance of appropriate Data Security levels is obtained by one team and this approach also helps with accountability. With this in mind it is important that the IT team is integrated into the procurement and planning process of any technical project which will embrace data collection online. No online service or application should be approved without formal sign off from the Head of Facilities and IT. The ICO has issued guidance around this area: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

14. Subject Access Requests ("SARs")

Overview

14.1 Data subjects have a right to access any personal data about them that Amnesty holds subject to certain exemptions.

14.2 A SAR can only be made by or on behalf of a data subject. A relative of a data subject does not have the right to see the personal data that Amnesty holds about that person, unless they can demonstrate that they are acting on behalf of the data subject (see section 14.10).

14.3 The process for responding to a subject access report is as follows:

14.3.1 Log the request and notify the Data Protection Compliance Officer;

14.3.2 Send a holding response letter;

14.3.3 Check identity of data subject who is making the request or on whose behalf the request is being made (see section 14.9);

14.3.4 Locate personal data;

14.3.5 Obtain approval of Data Protection Compliance Officer;

14.3.6 Send personal data which needs to be disclosed and update log.

14.4 Note that only the organisation which receives a SAR is required to respond to it. For instance, if UK Section receives a request, personal data held by UK Trust which is not also held by UK Section does not need to be disclosed. This may be helpful in some circumstances, although in many cases it will be difficult to say definitively that personal data is held by one Amnesty entity but is not held by the other. Where a request is made of either UK Section or UK Trust, only the entity receiving the request needs to respond, even if the other entity also holds personal information about the person making the SAR.

What Information does Amnesty need to disclose on receiving a SAR?

14.5 Amnesty is only obliged to disclose "personal data" in response to a SAR. As explained in the definitions section, personal data is information that relates to a living individual who can be identified from that data alone or from that data and any other information which is in the possession of Amnesty. Amnesty should consider carefully whether the information has any biographical significance in relation to the individual, e.g. the fact that a person attended a meeting is personal data about that person, but does not mean that everything in the minutes of that meeting is personal data about that person. If you are unsure about whether information is personal data, please ask the Data Protection Compliance Officer.

14.6 Amnesty's response should include a copy of the personal data it holds about the person making the request and any information it has about where the information came from (if this is relevant). Amnesty should include an outline of the reasons why it holds the information and details of who else is likely to see it. In many cases, these will be self-explanatory (e.g. for HR purposes).

Will Amnesty need to search all of its records which hold information about the individual making the SAR?

14.7 The request must relate to information held in a form from which the person making the SAR can be identified. This will include information in:

14.7.1 hard copy which is held as part of a highly structured filing system (i.e. in a way which enables isolation of particular information about a particular individual);

14.7.2 in electronic format; or

14.7.3 in a format which is intended to be put into electronic format.

14.8 There is no obligation to disclose any other data. Currently, as a result of case law (as referred to in section 8.4), most data that is held only in physical hard copy form (as opposed to electronically) is likely to be held as a filing system which is insufficiently structured. Therefore, most paper documents will not need to be disclosed by Amnesty in response to a SAR. Amnesty should seek legal advice before relying on this exemption as best practice is for paper records to be disclosed if possible.

Does the law require individuals to make a request in a certain way?

14.9 An individual making a SAR must make the request in writing and enclose a fee of £10. Therefore if Amnesty receives a request by telephone, it can ask the individual to put the request in writing. Similarly if it receives a written request which does not enclose the fee of £10, it can contact the individual and ask them to provide this additional information/ money. The 40 calendar days time period does not start until Amnesty has received all of the necessary information and the fee.

What should Amnesty do to check the identity of the person making the request?

14.10 There must be sufficient information in the request to properly identify the data subject and to enable Amnesty to comply with the request. Amnesty is entitled to receive proof of such identity. It may, for example, ask for a certified copy of the person's passport or driving license. Again, the 40 calendar days period within which Amnesty has to respond will only start from the time it receives this necessary information.

14.11 A SAR can be made by an agent on behalf of a data subject (e.g. a solicitor). Where Amnesty receives a request from an agent, it should check that the agent has been properly authorised to make the request. If the agent has not provided any Amnesty should ask him or her to produce satisfactory evidence of authority. This might be by way of a letter of authority signed by the data subject.

Can Amnesty rely on any of the exemptions which apply to SARs?

Disproportionate effort

14.12 Amnesty is not obliged to disclose the data held if this would involve a disproportionate amount of effort. Most information held on computers can be found by a search function and will rarely fall into this exemption. Amnesty should not seek to rely on this exemption without taking legal advice.

Previous compliance with same or similar request

14.13 If Amnesty has already complied with the same or a similar request from the individual recently, there is no obligation to comply with the new request. This can be used to assist Amnesty with persistent vexatious requests.

Disclosure which will involve also disclosing information relating to another person

14.14 Amnesty is not obliged to comply with the request if doing so would also disclose information relating to another individual, unless that individual has consented, or it is reasonable to disclose the information even if the other individual does not consent.

14.15 Whether such disclosure would be 'reasonable' will depend on any duty of confidentiality owed to the other individual, any steps Amnesty has taken to seek their consent, whether they are capable of consenting, and whether they have expressly refused consent.

14.16 Even if an individual refuses such consent Amnesty should conduct a 'balance of harm' test and consider whether not disclosing the information could harm the individual making the request more than the harm that would be caused to the third party if the information was disclosed.

Statutory Exemptions

14.17 If the information relates to crime, taxation, health, education, social work, regulatory activity, journalism or artistic activities then a statutory exemption may apply. Similarly if the data relates to ongoing negotiation with the data subject, or has been obtained in connection with legal proceedings, Amnesty may not need to disclose it. Amnesty should take legal advice where one of these exemptions might be relevant.

14.18 References given by Amnesty for specified purposes (education, training or employment, appointment to office or provision of any service) are exempt from subject access. References received by Amnesty from a third party may also be exempt; the balancing test relating to third party information should be applied to third party references (see sections 14.12 to 14.14).

What should Amnesty do if it seeks to rely on one of the exemptions above?

14.19 If the data requested is exempt from disclosure for any of the reasons outlined above, Amnesty should write to the applicant and explain that the information requested is exempt from disclosure and refer to the applicable exemption.

If Amnesty does need to disclose some information to an applicant, how long does it have and how should it do this?

14.20 Where information must be disclosed, Amnesty should send a letter of disclosure within 40 calendar days after the written request, fee, and proof of identity have all been received. The letter should identify the personal data held, explain the purposes for which that data is being processed (in general terms – e.g. "for direct marketing"), and describe the category of person to whom it may be or has been disclosed. It is usually appropriate to state that some or all of the disclosed data is confidential information and that the recipient is not authorised to release such information to anyone else. A copy of all information that is not confidential or exempt from disclosure for any other reason should be provided to the data subject.

What remedies will individuals have against Amnesty if it does not comply with their request?

14.21 If an individual is not satisfied that the request has been properly complied with, they can make a complaint to the ICO. The ICO can require further information from Amnesty in order to be satisfied that it has acted in accordance with the DPA, and if the ICO is not satisfied it can order disclosure.

14.22 The individual making the request also has the right to take the matter to court, to obtain an order requiring Amnesty to comply with their request for disclosure where Amnesty has not complied with its legal obligations.

Further information

14.23 For a quick summary of how to deal with SARs, please see the flow chart at Appendix D. For further information on how to deal with SARs, please contact the Data Protection Compliance Officer.

15. Guidance for employee data

Capturing Data during Recruitment

Application for employment

15.1 Applicants are made aware of what information will be held about them and what will happen to it should they be unsuccessful.

15.2 Amnesty should use a standard application form that does not ask for sensitive personal data (except on a separate, voluntary equal opportunities monitoring form). This is made clear using a data protection statement:

Data protection statement

In submitting this application, I agree that Amnesty may collect the personal data it contains and use that data for recruitment, human resource management and training purposes only. In the event that my application is unsuccessful, I understand that my details will be securely destroyed after six months.

Verification of recruitment data

15.3 Where information is obtained in the course of verifying the details supplied by an applicant or in the course of pre-employment vetting, we do not use the information for any other purpose. Once verification is complete, we destroy the information, merely keeping a record that verification has been carried out and the result.

Signing a contract of employment

15.4 Newly appointed staff should be informed what information will be kept about them, where it is obtained from, how it is used and who will have access to it. Explicit consent should be obtained for any sensitive personal data kept although such consent is not necessary when the information is required by Amnesty to comply with statutory obligations such as health and safety laws.

Data held on employees

15.5 The list of documents that HR routinely holds on staff is listed in Appendix C to this policy.

15.6 ***Personal Development Review*** Our Personal Development Review system is operated in accordance with accepted good practice to ensure personal information is obtained and used fairly and lawfully.

Any staff member may see the information recorded in the Personal Development Review system about them. Please arrange this with Human Resources.

Accuracy of employee data

15.7 We take steps to ensure that the personal records we keep are accurate and up-to-date and will correct any inaccuracies that are identified.

Monitoring

15.8 We may monitor internet usage in accordance with the internet usage policy.

Access to employee data

Access to your personal data

15.9 To access the personal data we keep about you, please ask Human Resources. They will arrange a mutually convenient time for you to view the contents of your file or data held about you on the HR database.

15.10 They will aim to make this date within a working week, subject to staff availability. As the file is the only record of some data, you cannot take it away, but Human Resources can provide you with a copy of any of the documents held on it. They will show you as much as we are allowed to under the law.

15.11 You are responsible for ensuring that any personal data held by you is kept securely. This includes appropriate use of computer user ids and passwords.

16. Local Groups and other affiliated organisations

We do not consider that local groups or other groups affiliated with Amnesty (such as Associate Members, Youth Groups and Student Groups) are bound by this policy as they are separate organisations. However we encourage these groups to be aware of their obligations under data protection legislation. If you have any queries about Amnesty's authority to share information with Amnesty Groups, please see Appendix G.

17. Notification

17.1 The organisation's data protection notification defines our data subjects (i.e. the people about whom we hold personal data), our data categories (the information we hold about them) and our purposes (the reasons why we hold this information). A copy of our notification may be viewed on request, or online via the public register on the web site of the ICO (www.informationcommissioner.gov.uk).

17.2 Processing which is not included in our Notification (additional purposes or types of information) should not take place. The Notification is reviewed once a year to ensure it is still accurate and up to date. If you think we are, or should be, processing data that is not covered by our Notification, please tell the Data Protection Compliance Officer immediately.

Appendix A

Human Resources Records

Your human resources file will typically contain the following documents/ information:

1. The job advert for the post you were appointed to.
2. The application form you signed updated for any role you have been appointed to.
3. Amnesty's offer letter to you and a statement of employment particulars, signed by you.
4. A document showing how you comply with Asylum and Immigration Act and your right to work in UK. This will be your passport, visa or ID card.
5. References provided by third parties.
6. Your personal details form and completed medical clearance letter.
7. Documents affecting your terms and conditions/confirming contractual changes after appointment e.g. pay rises, increments, hours changes, leave of absence. These will confirm the rationale/basis for the decision e.g. a minute of a management decision for change or new post, a signed flexible working agreement, etc.
8. Signed Appraisal review documents.
9. File notes of any discussions or telephone calls with or involving you.
10. Self-certification forms, medical certificates from a doctor or other practitioners.
11. Doctor's report(s) and any correspondence with a medical adviser/practitioner and you, under absence management processes.
12. Where appropriate, disciplinary and capability (competence) documents – if any formal action has been taken, then calls to hearing, notes taken at hearing and letter to confirm outcome of hearing.
13. Maternity: Amnesty's acknowledgement letter, your confirmation of child's birth date.
14. Your resignation letter, Amnesty's acknowledgement of your resignation, or a letter from Amnesty terminating your employment on other grounds.
15. Copies of any references written after employment. If you write a reference on behalf of Amnesty, you should be aware that these are disclosable to the data subject.
16. Any documents concerning legal action after employment has ended – unless they are covered by legal privilege, in which case, they will be withheld.
17. Pension details.

Amnesty will also hold other human resources/financial information relating to you in its finance department including:

18. Union subscription: your signed agreement for payroll deduction (most recent only)
19. Loans: your signed loan requests, where appropriate and information about outstanding loans.
20. Expenses and other claims for re-imbursement

Appendix B

Data Retention Policy

It is a requirement under the DPA that data should not be kept longer than purposes require. The DPA does not specify what this period of time should be. This means there are no legally enforceable timescales for retention and deletion of personal data. These are guidelines only and presuppose that consent has been obtained (where necessary).

Supporter Records

The table below shows guidelines for retention of supporter records.

Supporter Records Retention	
Name & Address Details	6 years
Banking Details	Until stop request received
Credit Card Details	Until stop request received
Telephone Preference Service suppression request	Indefinitely
"No Swaps" request	Indefinitely
Email address	3 years
Email Opt In request for Campaigns	Until campaign end date
Date of Birth	To be kept until supporter reaches age of 18 (unless there is a reason to keep it for longer)
Other information	6 years

Employee Records

The table below shows the Amnesty's guidelines for retention of employee and (where relevant) volunteer records.

Employee Records Retention	
Recruitment records for unsuccessful applicants (not shortlisted)	6 months from date applicants are informed that they have not been shortlisted, unless consent otherwise obtained and given
Recruitment records for unsuccessful applicants (shortlisted)	4 months from date applicants are informed of the decision, unless consent otherwise obtained and given
Application form/CV	Duration of employment
References received	Duration of employment and archived after termination of employment (for 6

Employee Records Retention	
	years)
Payroll & tax information	6 years (in addition to the year an employee commences employment)
Sickness records	6 years
Annual leave records	[Duration of employment and archived for 6 years after termination of employment]
Unpaid leave/special leave records	Duration of employment and archived for 6 years after termination of employment
Annual appraisal/assessment records	6 years
Records relating to promotion, transfer, training, disciplinary matters	6 years from end of employment
References given/information to enable reference to be provided	6 years from reference/end of employment
Summary of record of service (e.g. name, position held, dates of employment)	10 years from end of employment
Records relating to accident or injury at work	12 years

Financial Records

The table below shows the Amnesty's guidelines for retention of finance records.

Finance Records Retention	
Payments cash book or record of payments made	6 years from the end of the financial year in which the transaction was made
Invoice - revenue	6 years from the end of the financial year in which the transaction was made
Petty cash records	6 years from the end of the financial year in which the transaction was made
Invoice – capital item	10 years
Bank statements	6 years from the end of the financial year in which the transaction was made
Correspondence re donations	6 years from the end of the financial year in which the transaction was made
Gift Aid declarations	6 years after the last payment made or 12 years if there is a dispute regarding gift

Finance Records Retention	
Purchase orders	6 years from the end of the financial year in which the transaction was made
Contracts with suppliers and others	6 years after contract has come to an end

Visitor Records

Records of the names and addresses of individuals visiting Amnesty's offices are retained for 3 years from the date on which the information is collected.

Appendix C

Data Processing Agreement

Dated 2015

[Amnesty International UK]

and

[Data Processor]

Agreement with Data Processor

Bates Wells & Braithwaite London LLP
2–6 Cannon St
London EC4M 6YH
Ref: 010923/0054/MOR

Agreement

Dated: 20[15]

Parties:

[Insert name and relevant details of Amnesty entity acting as data controller]]

(the "Data Controller")

and

[Insert name and relevant details]

(the "Data Processor")

Background

The Data Controller uses the services of the Data Processor from time to time [*insert activity, e.g. carry out mailings/marketing/data cleaning services etc]*.

The Parties have agreed to enter into this Agreement to ensure compliance with the Data Protection Act 1998 in relation to all such processing.

The terms of this Agreement are to apply to all data processing carried out for the Data Controller by the Data Processor and to all personal data held by the Data Processor in relation to all such processing whether such personal data is held at the date of this Agreement, has been held prior to the date of this Agreement or is or received afterwards.

Interpretation

18. The terms and expressions set out in this agreement shall have the following meanings:

18.1 "Act" means the Data Protection Act 1998;

18.2 "Contract" the [service] agreement between the parties dated [*insert date*];

18.3 "Data Controller", "Data Processor" and "processing" shall have the meanings ascribed to them in the Act;

18.4 "ICO" means the Information Commissioner's Office; and

18.5 "Personal Data" shall include all data relating to individuals which is provided to the Data Processor by the Data Controller and/or which is or has been processed by the Data Processor on behalf of the Data Controller in accordance with this Agreement or at any time prior to the date of this Agreement.

It is agreed as follows:

19. This Agreement sets out various obligations in relation to the processing of data under the Contract. If there is a conflict between the provisions of the Contract and this Agreement, the provisions of this Agreement shall prevail.

20. The Data Processor is to carry out [*describe services as in (A) above*] and process Personal Data only on the express instructions of designated contacts at the Data Controller (which may be specific instructions or instructions of a general nature as set out in the Contract or as otherwise notified by the Data Controller to the Data Processor during the term of the Contract).

21. The Data Processor shall comply at all times with the Act and shall not perform his obligations under the Contract in such way as to cause the Data Controller to breach any of its applicable obligations under the Act.

22. All Personal Data is strictly confidential and may not be copied, disclosed or processed in any way without the express authority of the Data Controller.

23. The Data Processor agrees to comply with any reasonable measures required by the Data Controller to ensure that its obligations under this Agreement are satisfactorily performed in accordance with all applicable legislation from time to time in force and any best practice guidance issued by the ICO.

24. Where the Data Processor processes Personal Data (whether stored in the form of manual or electronic records) it shall:

24.1 process the Personal Data only to the extent, and in such manner, as is necessary in order to comply with its obligations under the Contract or as is required by law or any regulatory body including but not limited to the ICO;

24.2 implement appropriate technical and organisational measures and take all steps necessary to protect the personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure;

24.3 in furtherance of its obligations under 7.2 above implement and maintain the security measures set out in Schedule [1] to this agreement;

24.4 if so requested by the Data Controller (and within the timescales required by the Data Controller) supply details of the technical and organisational systems in place to safeguard the security of the Personal Data and to prevent unauthorised access to it;

24.5 on reasonable prior notice, permit persons authorised by the Data Controller to enter into any premises on which Personal Data is processed and to inspect the Data Processor's systems to ensure that sufficient security measures are in place;

24.6 notify the Data Controller (within two working days) if it receives:

24.6.1 a request from a data subject to have information about, or access to that person's Personal Data; or

24.6.2 a complaint or request relating to the Data Controller's obligations under the Act;

24.7 provide the Data Controller with full co-operation and assistance in relation to any complaint or request made, including by:

24.7.1 providing the Data Controller with full details of the complaint or request;

24.7.2 complying with a data access request within the relevant timescale set out in the Act and in accordance with the Data Controller's instructions;

24.7.3 providing the Data Controller with any Personal Data it holds in relation to a data subject (within the timescales required by the Data Controller);

24.7.4 providing the Data Controller with any information requested by the Data Controller;

24.8 not process Personal Data outside the European Economic Area without the prior written consent of the Data Controller and, where the Data Controller consents to a transfer, to comply with the obligations of a Data Controller under the Eighth Data Protection Principle set out in Schedule 1 of the Act by providing an adequate level of protection to any Personal Data that is transferred;

24.9 not transfer or disclose any Personal Data to any third party without the written consent of the Data Controller and ensure that any third party to which it sub-contracts any processing has entered into a written contract with the Data Processor which contains all the obligations that are contained in this Agreement and which permits both the Data Processor and the Data Controller to enforce those obligations.

25. The Data Processor shall transfer all Personal Data to the Data Controller on the Data Controller's request in the formats, at the times and in compliance with the specifications set out in Schedule [2].

26. The Data Processor shall be liable for and shall indemnify (and keep indemnified) the Data Controller against each and every action, proceeding, liability, cost, claim, loss, expense (including reasonable legal fees and disbursements on a solicitor and client basis) and demand incurred by the Data Controller which arise directly or in connection with the Data Processor's data processing activities under this Agreement (including all such activities undertaken before the date of this Agreement), including without limitation those arising out of any third party demand, claim or action, or any breach of contract, negligence, fraud, wilful misconduct, breach of statutory duty or non-compliance with any part of the Act by the Data Processor or its employees, servants agents or sub-contractors.

27. The Data Processor agrees that in the event that it is notified by the Data Controller that it is not required to provide any further services to the Data Controller under this Agreement, the Data Processor shall transfer a copy of all information (including Personal Data) held by it in relation to this Agreement to the Data Controller in a format chosen by the Data Controller or, at the Data Controller's request, destroy all such information using a secure method which ensures that it cannot be accessed by any third party and shall issue the Data Controller with a certificate of secure disposal.

28. All copyright, database rights and other intellectual property rights in any Personal Data (including but not limited to any updates, amendments or adaptations to the Personal Data by either the Data Controller or the Data Processor) shall belong to the Data Controller. The Data Processor is licensed to use such data only for the term of and in accordance with this Agreement.

29. [The Data Processor accepts the obligations in this Agreement in consideration of the Data Controller continuing to use its services.

    or

    The Data Processor accepts the obligations in this Agreement in consideration of the payment of £1 from the Data Controller which the Data Processor hereby acknowledges.]

30. [Where the provisions of this Agreement conflict with any other agreement between the parties, the p*rovisions of this Agreement shall prevail.*][*Do not use if including Clause 1 above.*]

31. This Agreement shall be governed by the laws of England and Wales.

SIGNED for and on behalf of

[insert name of Amnesty entity which is entering contract]

Print Name: …….

Position: ……..

SIGNED for and on behalf of

[ ]

Print Name: ……..

Position: ……

Schedule 1
Security Measures to be adopted by the Data Processor

The Data Processor will ensure that in respect of all personal data it receives from or processes on behalf of the Data Controller it maintains security measures to a standard appropriate to:

the harm that might result from unlawful or unauthorised processing or accidental loss, damage or destruction of the personal data;

the nature of the personal data.

In particular the Data Processor shall:

have in place and comply with a security policy which:

2.1.1 defines security needs based on a risk assessment;

2.1.2 allocates responsibility for implementing the policy to a specific individual or members of staff;

2.1.3 is provided to the Data Controller on or before the commencement of this Agreement;

2.1.4 is disseminated to all relevant staff; and

2.1.5 provides a mechanism for feedback and review.

ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the personal data in accordance with best industry practice;

prevent unauthorised access to the personal data;

ensure its storage of personal data conforms with best industry practice such that the media on which personal data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to personal data is strictly monitored and controlled;

have secure methods in place for the transfer of personal data whether in physical form (for instance, by using couriers rather than post) or electronic form (for instance, by using encryption);

put password protection on computer systems on which personal data is stored and ensure that only authorised personnel are given details of the password;

take reasonable steps to ensure the reliability of any employees or other individuals who have access to the personal data;

ensure that any employees or other individuals required to access the personal data are informed of the confidential nature of the personal data and comply with the obligations set out in this Agreement;

ensure that none of the employees or other individuals who have access to the personal data publish, disclose or divulge any of the personal data to any third party unless directed in writing to do so by the Data Controller;

have in place methods for detecting and dealing with breaches of security (including loss, damage or destruction of personal data) including:

2.10.1 the ability to identify which individuals have worked with specific personal data;

2.10.2 having a proper procedure in place for investigating and remedying breaches of the data protection principles contained in the Act; and

2.10.3 notifying the Data Controller as soon as any such security breach occurs.

have a secure procedure for backing up and storing back-ups separately from originals; and

have a secure method of disposal unwanted personal data including for back-ups, disks, print outs and redundant equipment.

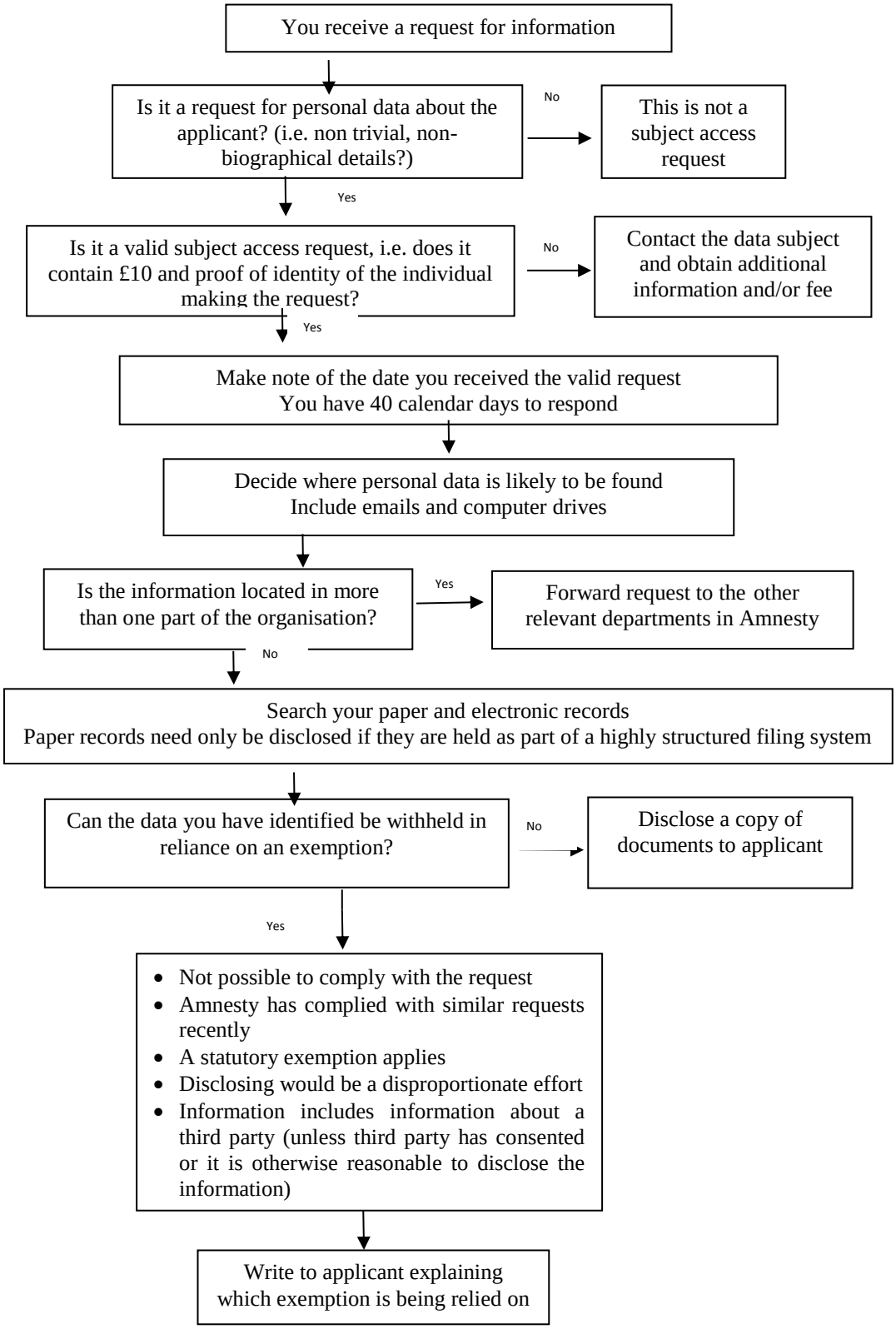
Schedule 2

Insert details relating to the transfer of data by the Data Processor to the Data Controller as set out in paragraph 8 of the Agreement, including:

- content of data to be transferred;
- format of the data; and
- timings for transfers.

Appendix D

Subject Access Flowchart



Appendix E

Model Statements for Data Collection

1. **Basic Statement**

Name:

Address:

Mobile: (for calls and SMS messaging)

Email address:

Confirm email address:

1.1 **Print Version**

We would love to keep you informed. We will send you updates about Amnesty's work. Other Amnesty groups in your area may also contact you.

1.2 "*I would like to receive email updates about the activities of Amnesty Groups in my area.*"

If this is not correct, please write no here.____

If at any time you prefer not to receive updates from Amnesty*, or our groups in your area please contact us [using the enclosed freepost envelope] [at Amnesty International UK, Supporter Care Team, 17-25 New Inn Yard, London, EC2A 3EA], by telephone 020 7033 1777 or email sct@amnesty.org.uk, specifying which updates you do not wish to receive.

1.3 **Online Version**

We would love to keep you informed.

1.3.1 ☑ I would like to receive updates about Amnesty's work

1.3.2 ☑ I would like to receive updates from other Amnesty groups in my area

Please untick if these statements are not correct.

If at any time you prefer not to receive updates from Amnesty*, please email sct@amnesty.org.uk specifying which updates you do not wish to receive.

Amnesty is the collective name for Amnesty International (UK Section) Charitable Trust, registered charity 1051681, company number 3139939 and Amnesty International United Kingdom Section, company number 1735872, both of which may use the information you provide. In both cases, the registered office is at 17-25 New Inn Yard, London, EC2A 3EA.

1.4 Tick here if you do not wish to receive postal communications from other carefully selected organisations ☐

We care about your details and unless you have agreed on this form we will never share your phone number or email address. Amnesty will not share the contact details of under 18s.

1.5 So that we can ensure that you receive appropriate communications, if you are under 18, please tell us your date of birth [**collect date of birth**].

1.6 For more information about how Amnesty processes personal data, see our privacy policy at www.amnesty.org.uk/privacy.

2. **Explanatory notes to basic statement – *please read these in conjunction with Amnesty's data protection policy***

2.1 A collection statement must always be used when collecting personal information from individuals for the first time. The statement above is Amnesty's starting point. Variants may be used as explained below or as otherwise agreed with the Head of Supporter Relations.

2.2 The numbering is included for ease of reference only. You do not need to number the separate sections when using this statement.

2.3 Section 1.1 informs people that Amnesty will share their information with other Amnesty Groups. Please note that this does not permit groups to contact individuals *by email*. You should only share a supporter's email address with an Amnesty Group where that supporter has not inserted the word "no" in section 1.2.

2.4 If you are enclosing a freepost envelope with the data collection statement, you should delete Amnesty's postal address from section 1.2.

2.5 Where supporters do not want to receive updates from Amnesty, the statement asks them to contact Amnesty to make this known. You do not need to include a tick box opt-out. If, because of the nature of your campaign, you would rather allow people to opt into receiving updates or other communications (i.e. only receive information from Amnesty and its groups where they have taken a positive step to request it), please replace the wording in section 1.2 with the wording below. Please note Amnesty expects this varied wording to be used only in exceptional circumstances.

Please tick the statement below if you would like Amnesty to keep you informed.*

"☐*I would like to receive updates about Amnesty's work.*

2.6 Where individuals have not unticked either of the boxes in the online version of the statement, Amnesty may share their contact details (including email addresses) with Amnesty Groups. Where an individual has unticked either box, you should record their preference clearly so that their request is respected.

2.7 The basic statement does not allow any third parties with whom Amnesty may share data to contact individuals by email for marketing purposes, e.g. to send updates by

email. It does however permit postal details to be shared provided the tick box in section 1.4 remains unticked.

2.8 It is important when collecting individuals' information to ensure the data contains clear fields indicating what preferences they have expressed in relation to:

2.8.1 receiving postal mailings and other information from Amnesty and Amnesty Groups;

2.8.2 receiving email marketing/information from Amnesty;

2.8.3 receiving postal mailings from unrelated third parties, e.g. other charities or commercial organisations;

2.8.4 receiving email/marketing information from other Amnesty Groups.

3. **Shorter statement to ensure minimum compliance**

Where space is limited, please use the following statement:

3.1 *By giving us your details, you are also requesting updates about Amnesty's work and the work of Amnesty Groups in your area.*

Email address:

3.2 *So that we can ensure that you receive appropriate communications, if you are under 18, please tell us your date of birth [collects date of birth].*

3.3 *If at any time you prefer not to receive updates from Amnesty, please tell us: www.amnesty.org.uk/contact.*

Print version - email

3.4 *"I would like to receive updates from Amnesty Groups"*

If this is not correct, please write "no" here:……:

Online Version

3.5 *I would like to receive updates from Amnesty Groups in my area ☑ (please untick if this is incorrect)*

3.6 Tick here if you do not wish to receive postal communications from other carefully selected organisations ☐

**Amnesty is the collective name for Amnesty International (UK Section) Charitable Trust, registered charity 1051681, company number 3139939 and Amnesty International United Kingdom Section, company number 1735872, both of which may use the information you provide. In both cases, the registered office is 17-25 New Inn Yard, London, EC2A 3EA.*

4. **Explanatory notes to shorter statement**

4.1 This statement is intended to ensure minimum compliance only. Where space allows, when first collecting individuals' information, you should use the full statement set out in Section 1.

4.2 You should always include section 1.5 if targeting non-supporters.

5. **Statement to use when collecting sensitive personal data**

5.1 If you are collecting sensitive personal data (see 6 below for definitions) from individuals, please replace the statement relating to use of personal data by Amnesty in sections 1.2, 1.3 and 3.1 with the statement below.

5.2 *"Please tick the box below if you would like Amnesty to keep you informed.*

5.3 ☐ *I am happy for Amnesty to use any of this information I provide on this form to give me information about Amnesty campaigns, fundraising and events as well as other information that it thinks I might be interested in including information from Amnesty groups in the UK. "*

6. **Explanatory notes to sensitive personal data statement**

6.1 You should use the statement above if you are collecting any of the following information about individuals:

6.1.1 Political opinions

6.1.2 Health (physical or mental)

6.1.3 Membership of a trade union

6.1.4 Sexuality

6.1.5 Ethnicity

6.1.6 Criminal record (including alleged commission of any offence)

6.1.7 Religious or similar beliefs

6.2 This is because, to process sensitive personal data about an individual, in many cases you will need the explicit consent of the individual to anything that you are doing with their information. The individual should understand clearly how their information is being used. Amnesty should not rely on implied consent where it is collecting sensitive personal data.

6.3 You should never share sensitive personal data about individuals with third parties without speaking to the Data Protection Compliance Officer.

7. **Viral Marketing**

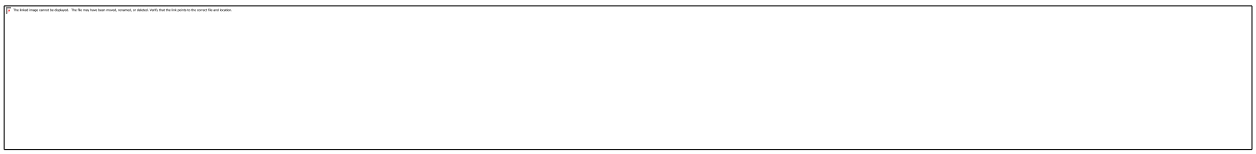
7.1 Before engaging in any viral marketing campaign, you should consult section 10 of Amnesty's data protection policy.

If you have any questions on these sample statements, please contact the Data Protection Compliance Officer.

Appendix F

Model Consent Forms for Photographs and other Recordings

To be used when recording images/taking photographs of under 14s



Amnesty International United Kingdom Section
Human Rights Action Centre, 17-25 New Inn Yard, London, EC2A 3EA

[EVENT NAME & ADDRESS] [EVENT DATE]

Dear Parent/Guardian

Amnesty† wishes to use creative material for its campaigning and fundraising (for example on its website or in publicity), which might include images or recordings of your child/the child in your care.

It is Amnesty's policy to use pictures and videos of young people under the age of 14 only where it has obtained permission from a parent or guardian. We would therefore be grateful if you could fill in the consent form below as appropriate.

If you wish to withdraw consent to an image being used in future or have any questions please email the Education & Student Team at: student@amnesty.org.uk

By completing this form, you agree to the following:

1. ***You consent to the creation of video, audio, photograph or other recording featuring your child/the child in your care and give all necessary licences and consents which may be required anywhere in the world (whether now or in future) to enable Amnesty to use it in all formats and in publications, websites, products and programmes.***
2. ***You assign to Amnesty any copyright or other rights in relation to the creation of video, audio, photograph or recordings in which your child/the child in your care is identifiable.***
3. ***Amnesty will process any video, audio or other images in which your child/the child in your care is identifiable in accordance with its Data Protection Policy and Child Protection Policy. For a copy of either policy, please contact sct@amnesty.org.uk.***

† *Amnesty is the collective name for Amnesty International (UK Section) Charitable Trust, registered charity 1051681, company number 3139939 and Amnesty International United Kingdom Section, company number 1735872, both of which may use the information you provide. In both cases, the registered office is 17-25 New Inn Yard, London, EC2A 3EA*

Please complete the fields below:

Parent/Guardian:

First Name:

Last Name:

Email address:

…… ……./……../……...

[Signature of parent/guardian:] **Date:**

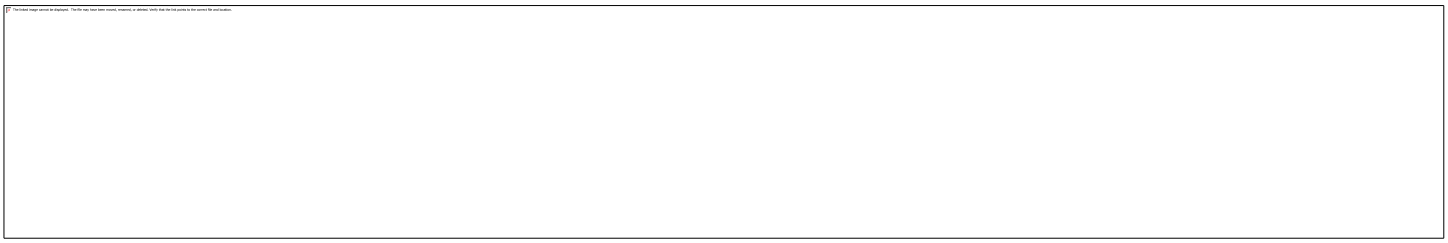
Name of young person:

First Name:

Last Name:

Date of Birth:

To be used when recording images/taking photographs of over 14s



Amnesty International United Kingdom Section
Human Rights Action Centre, 17-25 New Inn Yard, London, EC2A 3EA

[EVENT NAME & ADDRESS]
[EVENT DATE]

Photography/Filming/Recording Consent and Release Form
Age 14+

Amnesty[‡] wishes to use creative materials for its campaigning and fundraising (for example on its website or in publicity) which may include images or recordings of you.

By completing this form, you are agreeing to the following:

1. ***You confirm that you are aged 14+. If you are under 14, please ask your parent or guardian to sign the [ ] form.***

2. ***You consent to the creation of video, audio, photograph or other recordings featuring you and give all necessary licences and consents which may be required anywhere in the world (whether now or in future) to enable Amnesty to use it in all formats and in publications, websites, products and programmes.***

3. ***You assign to Amnesty any copyright or other rights in relation to the creation of video, audio, photograph or recordings at the above event in which you are identifiable.***

4. ***For your reassurance, Amnesty has a Data Protection Policy which will apply to all users described above. For a copy of the policy please contact sct@amnesty.org.uk***

If you wish to withdraw consent to your image being used in future publications or have any questions please contact the Supporter Care Team at: sct@amnesty.org.uk

[‡] *Amnesty is the collective name for Amnesty International (UK Section) Charitable Trust, registered charity 1051681, company number 3139939 and Amnesty International United Kingdom Section, company number 1735872, both of which may use the information you provide. In both cases, the registered office is 17-25 New Inn Yard, London, EC2A 3EA*

Please complete the fields below:

First Name:

Last Name:

Email address:

Date of Birth (if you are under 18)

…… ……./……../……...

[Signature] **Date**

Appendix G

FAQs on sharing personal data with Amnesty Groups

This guidance is intended for:

- Representatives of Amnesty Groups who seek guidance on notification with the ICO and sharing personal data with Amnesty and other Amnesty Groups; and
- Representatives of Amnesty who seek guidance on data sharing between Amnesty and Amnesty Groups.

1. **Do Amnesty Groups need to notify (i.e. register) with the Information Commissioner's Office?**

Short answer: In most cases, no.

1.1 **Longer answer**: In general, the DPA requires all data controllers to register or "notify" with the ICO. Organisations that notify need to pay an annual fee to the ICO (in most cases £35). However there are some exceptions to the obligation to notify. One is for non profit-making organisations which carry out only a limited range of activities. Although this exemption is quite narrow and so unlikely to be of use to larger Not-for-Profits like UK Section or UK Trust, guidance we have received indicates that most smaller Amnesty Groups can rely on the exemption and avoid the need to notify.

1.2 In summary, the exemption applies where the processing of personal data:

1.2.1 is carried out by a not-for-profit organisation (in this case an Amnesty Group);

1.2.2 is carried out to establish and maintain membership and/or support for the group or provide activities for its members;

1.2.3 is information about:

i. past, existing or prospective members of the Amnesty Group;

ii. individuals who have regular contact with the Group; and/or

iii. anyone whose personal data it is *necessary* to process to establish and maintain membership or support of the group;

and relates to

iv. eligibility for membership of the Amnesty Group;

v. other information which it is necessary to process to establish and maintain membership or support of the group or to provide activities for its members.

1.2.4 does not involve disclosure of data to any third party other than:

i. with the consent of the person whose data is being disclosed; or

ii. where it is necessary to establish or maintain membership or support of the Amnesty Group, or provide activities etc.

1.2.5 does not involve keeping information after the relationship with that supporter/member has ceased unless this is necessary.

Can Amnesty Groups rely on the exemption?

1.3 For Local Groups, Amnesty believes that they can rely on the exemption and do not need to notify.

1.4 The ICO has accepted that even where Groups process information about people who are not their members or supporters, they may still rely on the exemption. [For instance, a Group may be writing to prisoners of conscience. This is not information about members or supporters of the Group but processing it is "necessary" as it is one of the activities for which people join a group and therefore will not cause the groups to fall outside the exemption.]

What if we are processing personal data, not only to support the Group, but to further Amnesty's work generally?

1.5 The ICO has also accepted that, if a Group is heavily dependent for its existence on its relationship with a central organisation (in this case Amnesty), any activity related to fundraising for the wider group, can be considered as falling within the permitted purpose of maintaining support for the Group.

We are still concerned that our Group may need to notify?

1.6 If you think that your Group cannot rely on the exemption and needs to notify with the ICO, please contact craig.humphries@amnesty.org.uk for clarification.

2. ***Can Amnesty share personal data of supporters and contacts with Amnesty Groups where it has used the model data collection statements contained in this policy?***

2.1 Yes. The data collection statement in Appendix E tells people that they may be contacted by Amnesty Groups and gives them a choice about whether they want to be contacted by Groups.

Postal contact details

2.2 Where you have collected supporters' information using the model statement, as long as supporters have not opted out of receiving information from Groups, their details can be shared with Groups. The Groups can then contact those supporters about their own activities.

Email addresses

2.3 Email addresses should only be shared with Groups where individuals have ticked the box opting into receiving email updates from Groups on the template statement.

3. ***Can Amnesty share personal data of supporters and contacts with Amnesty Groups where the model statements have not been used and supporters have not previously been informed that this sharing might happen?***

Postal contact details

3.1 Best practice is for Amnesty to share supporter data with Groups only where individuals have been informed that this may happen. However, many supporters do not differentiate in their minds between Amnesty and its groups. Amnesty therefore feels that the risk of upsetting supporters by this sharing is low.

3.2 Even though the risk of complaints is low, Amnesty tries at all times to be transparent with its supporters about how their information is being used. Therefore we recommend that if Amnesty wishes to share supporter data with Groups, without having told supporters in advance, the following two steps should be taken:

3.2.1 Amnesty Groups should inform people as soon possible after receiving their details from Amnesty that they are now holding their information (and that they received it from Amnesty) and the purposes for which they will use their information. This need not be done as a separate mailing, but can be contained within the next mailing to those people (for example as a footnote, though it should not be too small!)

3.2.2 Amnesty should, in its next correspondence with its supporters (e.g. newsletter) tell them that it may share their data with its Groups

Email addresses

3.3 Amnesty Groups should only send marketing emails to individuals where individuals have consented to receiving marketing from Groups or agreed to receive mailings generally (see section 9.3 of the policy). Groups cannot rely on consent that was given to Amnesty for Amnesty alone to use their data (because Amnesty Groups are separate entities and not part of Amnesty).

4. ***Can Amnesty Groups share personal data of supporters and contacts with Amnesty?***

4.1 There are two issues to bear in mind when considering this question: (a) whether this sharing is permitted generally by the DPA and the Regulations and (b) whether this sharing is likely to trigger a need for Amnesty Groups to notify with the ICO.

Is this sharing permitted by the DPA?

4.2 As with Question 3, this will depend on what Amnesty Groups told individuals when they collected their information. Ideally, Amnesty Groups should tell people when they first collect their information that their details are likely to be shared with Amnesty. Where Groups have not done this, Amnesty should tell supporters whose details it has received from Groups that it is now holding their data, having received it from an Amnesty Group. It should also explain how it intends to use their information. It should do this in its next communication with them. Amnesty Groups should also try to tell supporters and members in their next communication with them that they may share their data with Amnesty in this way. Please remember that Amnesty should not keep supporters' data (received from Groups) unless it has a clear reason to do so.

Will sharing data with Amnesty trigger a need to notify with the ICO?

4.3 As above, to rely on the exemption from notification Amnesty Groups need to avoid disclosing personal data of their supporters to third parties unless:

4.3.1 they have the consent of their supporters to the sharing; or

4.3.2 the disclosure is *necessary* to establish or maintain membership or support for the Amnesty Group or to provide activities for the Group's supporters or contacts. By sharing the details of their supporters with Amnesty, Amnesty Groups are technically sharing them with third parties (i.e. UK Trust and UK Section). To avoid triggering a need to notify, the law requires Groups to ensure either that they have consent from supporters to this sharing or that they can demonstrate that this sharing is *necessary*. This could be quite restrictive to comply with in practice.

4.4 Helpfully, the ICO has advised that where Groups have not managed to get consent to sharing, provided they make every reasonable effort to be open with members and supporters about how personal data will be processed and for what purposes, this is unlikely to lead to enforcement action by the ICO unless for some reason a significant number of complaints are received by the ICO.

Email addresses

4.5 Amnesty Groups could share supporters' email addresses with Amnesty. However Amnesty should only use those email addresses to send marketing where it is confident that this complies with section 9.3 of this policy.

5. ***Can Amnesty Groups share personal data with each other?***

5.1 [The same principles apply to this question as apply under questions 3 and 4 above. If Amnesty Groups wish to share personal data of supporters with other Amnesty Groups, they should inform supporters when they collect their information (or as soon as possible after collecting it) that their data might be shared in this way. If they have not done this, sharing data between Groups is unlikely to trigger complaints to the

ICO provided the Groups take the steps in paragraphs 3.2 above. [For email addresses Groups wouldl need to have the necessary consent before sending marketing materials to email addresses they have received from other Groups. (See section 9.3 of the policy)] *Gill to prepare suitable wording*

6. ***Can Amnesty share personal data with Regional Representatives?***

As Regional Representatives are essentially representatives of Amnesty Groups, sharing with them will be governed by the response to question 3 above.

7. ***Should Amnesty Groups share suppression requests with Amnesty?***

When an Amnesty Group receives a suppression request from a supporter or contact, it should share that request with the Supporter Care Team at Amnesty (sct@amnesty.org.uk) as soon as possible. Amnesty can then decide whether the suppression applies to Amnesty or the Group only. If the suppression request is wide enough to cover Amnesty, it should be registered by Amnesty on its database (MASCOT) within [2] days of being notified to Amnesty.

8. ***Should Amnesty share suppression requests with Amnesty Groups?***

8.1 When Amnesty receives a suppression request from a contact or supporter, it should, where possible, check whether that contact or supporter is also a member of an Amnesty Group. If the person making the suppression request is also a member of an Amnesty Group and Amnesty thinks that the suppression should extend to communications from the Group, Amnesty should inform the Group of the request.

8.2 Where it is not possible to determine whether a supporter is also a member of an Amnesty Group, you should inform the person making the suppression request that their information may still be held by other Amnesty entities. Where possible, please use the statement below:

> "*We acknowledge your request to unsubscribe from our mailing lists and have removed you with immediate effect from those lists where we have identified your name. If you also receive mailings from Amnesty Groups or networks, we regret that we cannot unsubscribe you form their mailing lists.*. You should contact them separately to unsubscribe from their communications"

Appendix H

CCTV Code of Practice for AIUK

Introduction

Closed circuit television (CCTV) is used in AIUK's Human Rights Action Centre. The system compromises 10 cameras. 9 are over entrance and emergency exit doors and 1 in the safe room with images relayed back to the basement server room and the [OM] and reception area. The images are recorded and stored digitally within a secure area with restricted access.

Objectives of CCTV system

The stated objectives of AIUK for the use of CCTV cameras are as follows:

- Prevention, investigation and detection of crime including theft and criminal damage
- Apprehension and prosecution of offenders including use of images as evidence in criminal proceedings
- Public, employee and contractors safety
- Maintaining security of premises

General Principles

- The system will be operated in accordance with all the requirements and the principles of the Data Protection Act 1998.
- The system will be operated fairly, within the law, and only for purposes for which it was established and as identified within the Code of Practice.
- The system will be operated with due regard to everyone's right to respect for his or her privacy.
- AIUK believes that there is a public interest in operating the system. However, it will guard against any negative impact the system may have by ensuring its security and the integrity of operational procedures.
- AIUK will regularly review whether the use of CCTV continues to be necessary and justified.
- CCTV should not generally be used to record conversations between members of the public or staff members as this is likely to be a serious invasion of privacy. Covert monitoring will only be justified in specific cases where openness could prejudice the prevention or detection of crime or the apprehension of offenders.

Responsibilities

The CCTV systems are the responsibility of AIUK. Day to day responsibility for managing the system lies with the Head of Facilities & IT. The Head of Facilities & IT is responsible for ensuring AIUK's compliance with the CCTV Code of Practice.

AIUK has a responsibility to let people know that it is carrying out CCTV surveillance. AIUK should display prominently placed signs notifying people of the presence of the CCTV system, why it is in place and details of who to contact with any queries about the system.

Maintenance of Systems

Cameras should be maintained and serviced at regular intervals with a service log kept. In the case of a damaged or broken camera the responsibility lies with the Head of Facilities & IT to see that repairs are undertaken.

Storing Images

Images will be stored for a period of 30 days maximum in a secure environment with restricted access. They must be stored in an environment which will preserve the quality of the images. After 30 days, unless AIUK has identified a need to retain the images for a longer period, the images will be erased permanently and securely.

If images are retained as evidence past this period then the following information should be recorded:

- Date they were identified as necessary to retain for longer than the 30 day period and separated from the other images and if applicable and disclosed to a third party
- Reason why they were identified. Any crime number associated with the images.
- Location (e.g. police station) where they will be held and a signature for the removal from the collector

Security

The security of all images should be protected in accordance with the data security requirements set out in AIUK's data protection policy. Particular regard should be had to the following:

- Access to control rooms and locations where images are stored must be strictly monitored and controlled.
- When images are transferred to third parties, they must be transferred securely using a courier or Royal Mail Recorded Delivery service. Images should be signed for on delivery and should never be transmitted electronically.
- Staff must not make copies of images without the express authority of the Head of Facilities & IT.
- Where any staff are found to have misused CCTV images or otherwise breached this code of practice, they will be sanctioned in accordance with AIUK's disciplinary policy.

Viewing Images

Access to images should be carefully restricted to the Head of Facilities & IT who will consider all applications for viewing. Viewing of images should take place in a restricted

area which the Facilities Manager agrees is sufficiently private and secure. Any requests for viewing should be made in writing to the Head of Facilities & IT who shall determine who is eligible to view the images. All images viewed should be documented with the following information:

- Date and time of viewing
- Name of person viewing images
- Name(s) of viewer(s)
- Reason for viewing
- Outcome of viewing

Access by Law Enforcement Agencies

Any requests for viewing by the police or other law enforcement agencies should be considered on a case by case basis. AIUK should not automatically disclose information requested by such organisations unless the organisation making the request has a warrant or court order. Amnesty should balance the interests of the organisation making the request against those of the individual concerned.

Any requests by the police or other law enforcement agencies should be referred to the Head of Facilities & IT in the first instance.

Access by Data Subjects

Any requests for viewing should be made in writing to the Head of Facilities & IT. Individuals in other departments who receive a request should forward it to the Head of Facilities & IT without delay. An appropriate administration fee may be charged (maximum £10.00). AIUK will have 40 days following the receipt of a subject access request to provide the information requested.

The individual should provide sufficient information to identify the images required, AIUK may require them to submit a photograph if they are involved in the images to enable AIUK to identify the correct images. If the Facilities Manager decides a request is not valid he or she should supply the following information to the Data Protection Compliance Officer:

- The identity of the individual making the request
- The date of the request
- The reason for refusing to supply the images requested
- The name and signature of the manager making the decision.

Images will only be released to the individual once the Head of Facilities & IT or Facilities Manager has reviewed them and deemed them appropriate to release. If the images compromise the privacy of other data subjects, they may be withheld. Where Amnesty determines that certain images should be disclosed in response to a subject access request, the images should be recorded on a CD/DVD and provided to applicants securely in that format.

For more information on complying with subject access requests, see AIUK's [internal guidance on this subject and data protection policy.

Review of Code of Practice

This code will be reviewed on an annual basis or when any changes or additions are made to the monitoring systems.

Checklist for users of limited CCTV systems monitoring small retail and business premises

	Checked (date)	Checked by	Date of next review
Notification has been submitted to the Information Commissioner and the next renewal date recorded			
There is a named individual who is responsible for the operation of the system			
A system has been chosen which produces clear images which law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required			
Cameras have been sited so that they provide clear images			
Cameras have been positioned to avoid capturing the images of persons not visiting the premises			
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed with the sign(s)			
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them			
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated			
Except for law enforcement bodies, images will not be provided to third parties.			
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as the request is made			

Regular checks are carried out to ensure that the system is working properly and produces high quality images.			

Appendix I

Notification Procedure for Data Security Breaches

1. **Introduction**

1.1 As explained in section 13 of this policy, Amnesty must ensure that it puts in place appropriate security measures against unauthorised or unlawful processing of the personal data it holds and against the accidental loss of or damage to that personal data.

1.2 Where there is a loss or theft of personal data or release or corruption of personal data, you must notify the Data Protection Compliance Officer immediately.

2. **Reporting**

2.1 Although the DPA does not require Amnesty to report data security breaches, it is best practice to report serious breaches to the ICO. The Data Protection Compliance Officer will decide whether a breach needs to be reported to the ICO. In making his decision, he will take the following factors into account:

2.1.1 the potential harm to data subjects which could arise from the breach; and

2.1.2 the volume of personal data lost, released or corrupted; and

2.1.3 the sensitivity of the data lost, released or corrupted.

3. **Potential harm**

3.1 Where there is significant actual or potential harm as a result of the breach, whether because of the volume of data, its sensitivity or a combination of the two, the breach should be reported.

3.2 Where there is little risk that individuals would suffer significant harm, for example because a stolen laptop is properly encrypted, or the information that has been lost, released or corrupted is publicly available information, there is no need to report.

4. **Volume of personal data**

4.1 A breach should be reported to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering harm. While the Data Protection Compliance Officer will consider the facts of each case it is expected that any breach involving information about 1000 people will be considered large.

4.2 Therefore, a breach involving the theft / loss of an *unencrypted* laptop computer or other *unencrypted* portable electronic / digital media holding names and addresses, and other details such as dates of birth of 1000 individuals should normally be reported.

4.3 A breach involving the theft / loss of a marketing list of 500 names and addresses or other contact details without further data would not normally need to be reported to the ICO, but each case will be considered individually by the Data Protection Compliance Manager.

4.4 Amnesty may find it is appropriate to report much lower volumes in some circumstances where the risk is particularly high perhaps because of the circumstances of the loss or the extent of information about each individual. If the there is any uncertainty as to whether to report or not, then the presumption should be to report.

5. The sensitivity of the data

5.1 There should be a presumption to report a breach to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial harm. This is most likely to be the case where that data is sensitive personal data (see clause 3.10 for definition of sensitive personal data). The loss or theft of as few as 10 records might need to be reported if the information is particularly sensitive.

5.2 For example, if a manual paper based filing system (or *unencrypted* electronic system) holding personal data relating to 50 named individuals and their financial records was released, this is unlikely to need to be reported.

5.3 If the names of Amnesty supporter records for the same number of individuals were released, without any bank details, and there were no special circumstances surrounding the loss, then this should not be reported.

6. Reporting serious breaches to the ICO

6.1 Serious breaches should be notified to the ICO by:

email: casework@ico.gsi.gov.uk; or

post to: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

The security breach notification form can be found here:
http://www.ico.org.uk/for_organisations/data_protection/lose.aspx

Guidance on how to manage a data security breach can be found here:
http://www.ico.org.uk/for_organisations/guidance_index/data_protection_and_privacy_and_electronic_communications.aspx#security

6.2 The notification should include details of:

6.2.1 the type of information and number of records;

6.2.2 the circumstances of the loss / release / corruption;

6.2.3 any action which has been taken to minimise / mitigate the effect on individuals involved where information has been lost / stolen / damaged including whether they have been informed of the breach;

6.2.4 how the breach is being investigated;

6.2.5 any remedial action which has been taken or will be taken to prevent future occurrence; and

6.2.6 any other information which may assist the ICO in making an assessment.

7. What will the ICO do when a breach is reported?

7.1 In the event that Amnesty notifies a breach to the ICO, the nature and seriousness of the breach and the adequacy of any remedial action will be assessed and a course of action determined. The ICO may:

7.2 record the breach and take no further action; or

7.3 investigate the circumstances of the breach and any remedial action. This could result in:

7.3.1 no further action;

7.3.2 a requirement for Amnesty to take steps to prevent further breaches;

7.3.3 formal enforcement action (i.e. a formal legal obligation to take steps to prevent further breaches);

7.3.4 where there is evidence of a serious, deliberate or reckless breach of the DPA, a monetary penalty notice requiring Amnesty to pay a fine of an amount determined by the ICO which could be up to £500,000.

7.4 Where a breach has been voluntarily reported to the ICO, this will be taken into consideration when deciding on the most appropriate course of action.

8. Will a reported breach be made public?

8.1 In its guidance, the ICO states that it does not have a duty to publicise security breaches not already in the public domain or to inform individuals who are affected by the breach. It will be Amnesty's responsibility to notify the individuals affected by the breaches (see section 9).

8.2 However, the ICO may recommend that the breach be made public where it is in the interests of the individuals concerned or there is a strong public interest reason for doing so.

8.3 Where the ICO takes regulatory action, its policy is to publicise that action unless there are exceptional reasons not to do so.

8.4 In most cases, we would not expect the ICO to take regulatory action unless:

8.4.1 Amnesty fails to take any recommended action;

8.4.2 The ICO has other reasons to doubt Amnesty's future compliance; or

8.4.3 there is a need to provide reassurance to the public. Such a need is most likely to arise where the circumstances of the breach are already in the public domain.

9. Notifying individuals of the breach

9.1 When a breach has occurred the Data Protection Compliance Officer should consider whether the individuals involved should be notified. Notification should only be made where there is a clear purpose for doing so. For example, when:

9.1.1 it will enable individuals who may be affected to protect themselves (i.e. by cancelling a credit card or changing a password);

9.1.2 there is a contractual requirement for Amnesty to notify the individuals involved;

9.1.3 notification may assist Amnesty to meet its security obligations with regard to the seventh data protection principle.

9.2 When deciding how to notify the individuals concerned (i.e. by email or telephone), the Data Protection Compliance Officer should take the urgency of the situation into consideration.

9.3 The information given to individuals when notifying them of a breach will depend on the nature and severity of the breach, however, it should usually include the following:

9.3.1 a description of how and when the breach occurred and what data was involved;

9.3.2 what Amnesty has already done to respond to the breach;

9.3.3 advice on how the individuals involved can protect themselves and how Amnesty can help;

9.3.4 contact details of how to access further information (i.e. a helpline number or section of the Amnesty website).