



INFORMATION SECURITY POLICY

Version 1 – August 2007

<http://www.bab.org.uk>

List of Contents

1	Preface	5
2	Introduction	6
2.1	Breakdown	6
2.2	Physical Security	6
2.3	Backups	7
2.4	Password Policies	7
2.5	Staff Training	8
2.6	IMPORTANT NOTICE	8
3	Assumptions	9
3.1	Members and members	9
4	Personal Accident and Professional Indemnity Insurance	10
4.1	Responsibilities	10
4.2	Inception	10
4.3	Update / Expansion	10
4.4	Archive / Deletion	10
4.5	Additional Information	10
5	Membership	11
5.1	Responsibilities	11
5.2	Inception	11
5.3	Update / Expansion	11
5.4	Archive	11
5.5	Deletion	11
6	Coaching	12
6.1	Responsibilities	12
6.2	Introduction	12
6.3	Inception	12
6.4	Update / Expansion	12
6.5	Archive	12
6.6	Deletion	12

7	The World Wide Web	13
7.1	Responsibilities	13
7.2	Introduction	13
7.3	Inception	13
7.4	Update / Expansion	13
7.5	Archive	13
7.6	Deletion	13
8	Insurance Claim	14
8.1	Responsibilities	14
8.2	Introduction	14
8.3	Claim Information Inception	14
8.4	Claim Information Update	14
8.5	Claim Archive	14
8.6	Claim deletion	14
9	CRB Management	15
9.1	Responsibilities	15
9.2	Introduction	15
9.3	Inception/acquiring of data	15
9.4	Updates/expansion of data	15
9.5	Archiving of Data	15
9.6	Deletion / disposal of data	16
9.7	Release of information to the individual	16
9.8	Release of information to third parties	16
10	Child Protection – Incident Management	17
10.1	Responsibilities	17
10.2	Introduction	17
10.3	Inception/acquiring of data	17
10.4	Updates/Expansion of data	17
10.5	Archiving of Data	17
10.6	Deletion / disposal of data	17
10.7	Release of information to the individual	17
10.8	Release of information to third parties	18

11	Child Protection – Disciplinary Issues	19
11.1	Responsibilities	19
11.2	Introduction	19
11.3	Inception	19
11.4	Update / Expansion	19
11.5	Archive	19
11.6	Deletion	19
11.7	Release of information to the individual or to third parties	19
12	Data Protection Information	20
12.1	Responsibilities	20
12.2	Introduction	20
12.3	Inception	20
12.4	Update / Expansion	20
12.5	Archive / Deletion	20
12.6	Additional Information	20
13	Other Disciplinary Issue - Management	21
13.1	Responsibilities	21
13.2	Inception /Update / Expansion	21
13.3	Archive / Deletion	21
14	General Requests - Access to Data	22
14.1	Responsibilities	22
14.2	Request for Access	22
15	Breach and Notification Process	23
15.1	Responsibilities	23
15.2	Detection and Investigation of Security Breaches	23

1 Preface

- 1.1 This document details the processes by which the British Aikido Board (BAB) controls information: both personal information and information forwarded for the public domain.
- 1.2 This document replaces the BAB Data Handling Procedure version 1.0.
- 1.3 The BAB is committed to the correct and legal handling of data.
- 1.4 To this end, the BAB has put into place guidelines for all its Member Associations detailing their legal responsibilities. These guidelines are available by download from the “downloads” section of the BAB web site: www.bab.org.uk
- 1.5 The BAB is registered with the Information Commissioner’s Office (ICO), formerly the Office of the Data Protection Registrar.

2 Introduction

2.1 Breakdown

2.1.1 This document details the life cycle of data held within this Association. It also determines the actions to be taken should a breach of the rules takes place.

2.1.2 There are a number of areas of that require coverage within this document. Each has its own dedicated chapter. These areas are:

- Personal Accident and Professional Indemnity Insurance
- Membership,
- Coaching,
- The World Wide Web,
- Insurance Claim,
- CRB Management,
- Child Protection – Incident Management,
- Child Protection – Disciplinary Issues
- Data Protection Information,
- Other Disciplinary Issue - Management,
- General Requests - Access to Data,
- Breach Process.

2.1.3 Data life cycles consist generally of five parts. Within each chapter will be a section on each of these life cycle parts. These are:

- Responsibilities (both organisational and individual),
- Inception (initial receipt of data),
- Update / Expansion (renewal / modification of data),
- Archive (data required for historical reasons but no longer of direct consequence),
- Deletion (destruction of data),
- Additional comments.

2.2 Physical Security

2.2.1 All reasonable physical security measures should be taken to ensure the physical security of the data commensurate with the sensitivity of the data.

- 2.2.2 The default method of physically storing paper and backup media is a locked filing cabinet. In certain situations, this may be enhanced but this will be raised wherever applicable.
- 2.2.3 Paper files are locked away in filing cabinets when not in use.
- 2.2.4 All electronic data held on computers is held securely: namely in a reasonably protected location on a computer system with reasonable up-to-date anti-virus software installed and up-to-date, anti-spam software installed.
- 2.2.5 It is required that any computer system housing BAB information is protected by a firewall.
- 2.2.6 All positions of office are voluntary. There are no formal “offices” for the BAB so it is not feasible to enforce the use of building alarms, however, best practice indicates that where possible or necessary, physical alarms are available and used.
- 2.2.7 The BAB Secretary keeps a list of all key information for filing cabinets in case of loss.
- 2.2.8 Shredding is only an acceptable way of disposal of media/paper records if a cross-cut shredder is used. The BAB mandates cross-cut shredding as its standard way of disposal.

2.3 Backups

- 2.3.1 Backups are taken on a regular basis. As a minimum, backups are taken on a monthly basis, although individual officers are required to ensure there is a valid backup of data taken before any paperwork input to the computer system is destroyed.
- 2.3.2 All backups are treated with the same level of secure handling as the original data: namely locked away and disposed of securely (shredded). All backups are held for the prescribed period of time (as per each chapter) and are disposed of securely by shredding.
- 2.3.3 Backups are **NOT** password protected. In this way, should there need to be a requirement to access an Officer’s backups and the Officer is absent, it can be done.

2.4 Password Policies

- 2.4.1 All computer system Operating Systems are locked by administrative password.
- 2.4.2 All user accounts to the relevant computer systems are controlled by password.
- 2.4.3 Where possible, access to any database is also restricted by additional password protection.
- 2.4.4 There are no guest login accounts available on any computer system housing BAB information. Only the relevant User ID can access the BAB data.
- 2.4.5 All passwords should be a minimum of 8 characters and should include upper case, lower case and numeric characters. It is recommended that one of the first 6 characters of the password is a “special character” (such as !"£\$%^&*()~@#}{[]+_-="). This increases the strength of the password.

2.5 Staff Training

- 2.5.1 All Officers of the BAB have been distributed with a copy of this document. Should additional training be required, the BAB Data Protection Officer is available to give advice.

2.6 IMPORTANT NOTICE

- 2.6.1 Should any **Subject Access Request** (the formal term for any request made by an organisation or individual for access to their data), the rules apply as per each chapter below. However, the following overarching principle takes precedence:

Should the Association and/or the individual be under investigation by the Police or security forces and you have been asked not to divulge the information by those said forces, you are NOT to divulge the information. Neither are you to divulge the fact that you have the data or that it is being used in part of any investigation.

This area is covered under Section 29.1 of the Data Protection Act 1998 as per the date of this document (July 2007).

In all cases, before responding to the requestor, the matter must be discussed with the BAB DPO and a formal decision be reached before acting on it.

3 Assumptions

3.1 Members and members

- 3.1.1 “Members” of the BAB consist of the physical Associations. Each Association is represented by the Head of the Association and an Association Representative.
- 3.1.2 “members” consist of the Association membership and Association assistants (who are generally, but not necessarily members of Associations but undergo CRB checking at an Association’s behest).

4 Personal Accident and Professional Indemnity Insurance

4.1 Responsibilities

4.1.1 This area is managed by the BAB Secretary.

4.2 Inception

4.2.1 Associations forward a form containing names and age categories of students to the BAB Secretary on a monthly basis, together with the relevant fee.

4.2.2 No personal information is included other than the above information; consequently the requirements for Data Handling are minimal.

4.2.3 The BAB Secretary collates the forms and forwards them to the insurance broker (currently Perkins Slade) for handling, together with the fee.

4.2.4 The BAB does not charge an administration fee for the forwarding of this information.

4.2.5 The Coaching Team are advised of any person requesting Professional Indemnity Insurance in addition to the Personal Accident Insurance.

4.3 Update / Expansion

4.3.1 Data is never updated. It is replaced annually.

4.4 Archive / Deletion

4.4.1 Copies of the forms are kept for **1 year**, after which they are destroyed by shredding.

4.5 Additional Information

4.5.1 Accident / Injury Management will be handled as a separate section (section 8).

5 Membership

5.1 Responsibilities

5.1.1 Membership is managed by the BAB Membership Secretary. There is additional support handled by the BAB Secretary.

5.2 Inception

5.2.1 The BAB has a Membership Committee that manages the Inception of new Associations.

5.2.2 All data pertaining to a proposed membership are held by the Membership Secretary on paper records and occasional electronic documents.

5.2.3 Should a new Member be admitted to the BAB (having met all the relevant criteria), all data is passed to the BAB Secretary as a living 'document set' and any data held by the Membership secretary is deleted.

5.2.4 Data is deemed to be accurate as the Association supply the original information and the relevant representatives sign to authorise the use of the data.

5.3 Update / Expansion

5.3.1 A change of information concerning the Association Membership Record is not common, other than contact details and the change of representatives. This information is held by the BAB Secretary on her secure computer system. Backups are kept securely by the BAB Treasurer.

5.4 Archive

5.4.1 Should a proposed new Member fail to be admitted to the BAB, all data is passed to the BAB Secretary and is held for **3 years** in Archive before being destroyed.

5.4.2 Should a current Member leave the BAB, the BAB Secretary will archive the information for **3 years** in Archive before being destroyed.

5.5 Deletion

5.5.1 Once the data has been in archive for the required period, it is securely deleted by shredding.

6 Coaching

6.1 Responsibilities

6.1.1 There are three people involved in Coaching. The BAB Coaching Administration Officer (BAB CAO), the BAB Coaching Development Officer (BAB CDO) and the BAB Communications Officer.

6.2 Introduction

6.2.1 The BAB CAO keeps a database history of all BAB qualified instructor's certification history. This data is never deleted.

6.2.2 A reduced down copy of this data is passed to the BAB Communications Officer on a regular basis to ensure that information published on the World Wide Web concerning instructors is accurate.

6.3 Inception

6.3.1 Once a person receives a coaching award, the award, together with the name of the individual and the name of the Association are registered in the Coaching Database. No other personal information is kept on this database.

6.3.2 However, the BAB also runs coaching courses. While a prospective instructor undergoes his/her training courses, the BAB CAO holds a training record is kept that includes minimal personal information: contact details etc.

6.4 Update / Expansion

6.4.1 A change to a qualification is in effect a new qualification and is handled as such.

6.5 Archive

6.5.1 Personal data is kept until the person completes his training or indicates that he/she no longer wishes to continue with the training, at which point, the data is archived for **1 year**.

6.6 Deletion

6.6.1 The only data to be deleted are interim records prior to qualification. These records are destroyed securely after their period of archive is reached.

7 The World Wide Web

7.1 Responsibilities

7.1.1 This area is managed by the BAB Communications Officer.

7.2 Introduction

7.2.1 The BAB has a web site. This site is managed by the BAB Communications Officer and his assistant.

7.2.2 The majority of the data published on this site is data already in the public domain and therefore does not require authorisation to publish. However, the Communications Officer reviews the public domain data on a regular basis (**minimum 1 year**) to ensure that the information is still accurate.

7.2.3 Contact details at club level generally are local instructors' names and a contact telephone number for the club. This may be a personal number but is offered by the relevant instructor freely (it is not a pre-requisite).

7.3 Inception

7.3.1 All Associations are invited by the Web Administrator to input/update the club information using the "Club Information and WWW Publication" form, available on the BAB web site.

7.3.2 This form is in two parts. The first part contains public domain information and requires no signature. The second part consists of personal information that the club instructor is willing to have published. The instructor whose details are being published must sign this part of the form to allow for public disclosure of the information into the public domain.

7.3.3 The Communications Officer holds the completed forms.

7.4 Update / Expansion

7.4.1 The Communications Officer is required every **2 years** to audit the web site in total to confirm and ensure that that all information held on the web site is accurate.

7.4.2 Any change to the club information is undertaken by the same form as inception. The data is updated on the web, the original paperwork shredded and the updated form filed.

7.5 Archive

7.5.1 N/A.

7.6 Deletion

7.6.1 Once notified of the cessation of a club, the Web Administrator (Communications Officer) deletes the data from the web site and destroys the paper record.

7.6.2 If an Association ceases to be a Member, all club records are deleted from the web site and the relevant paperwork shredded within **1 month** of notification.

8 Insurance Claim

8.1 Responsibilities

8.1.1 This area is managed by the BAB Secretary.

8.2 Introduction

8.2.1 It is required by the Insurance Company that any claim made be forwarded through the BAB Secretary.

8.2.2 Please note that Child Protection issues are handled in a completely different way.

8.3 Claim Information Inception

8.3.1 The Perkins Slade Claim Form has two purposes: it firstly identifies that an accident has taken place and secondly, indicates that there is theoretically the possibility of a claim being made. It is **not** an indication that there will automatically be a claim made against the relevant Association or the BAB.

8.3.2 There are actually two claim forms that must be completed: the Personal Accident Claim Form completed by the claimant, and the Incident Notification Advice Form, completed by the Club/Association official.

8.3.3 Completed claim forms are sent to the BAB Secretary for processing from the relevant Association via recorded or special delivery.

8.3.4 The information is copied and the originals forwarded to the Insurers via recorded or special delivery.

8.3.5 All copies are held securely by the BAB Secretary in case of postal failure.

8.4 Claim Information Update

8.4.1 Should additional information be forwarded to the BAB concerning a claim, the BAB Secretary will forward that information to the Insurer as per paragraphs 8.3.2 and 8.3.3.

8.4.2 The Insurer will keep the BAB Secretary apprised of all outstanding claims and their status.

8.5 Claim Archive

8.5.1 Once a Claim is deemed closed, the information held by the BAB will be held for the statutory legal period of time (**normally 3 years, but in the case of minors 3 years after their 18th Birthday**) prior to destruction.

8.6 Claim deletion

8.6.1 All paperwork held in a claim file that has exceeded the statutory holding period is shredded.

9 CRB Management

9.1 Responsibilities

9.1.1 The handling of all matters pertaining to CRB Checks is managed by the BAB Lead Child Protection Officer (BAB Lead CPO).

9.2 Introduction

9.2.1 The BAB is committed to its Child Protection Policy. As such, it is now policy that all BAB qualified Instructors undergo a CRB check.

9.3 Inception/acquiring of data

9.3.1 Each BAB Member Association is responsible for risk assessing and administering CRB checks according to the prevailing guidelines as issued by the CRB, TMG, CPSU and/or the BAB.

9.3.2 Information from individual CRB checks is only returned to the BAB's Lead CPO if there is disclosure information. This is done by way of a duplicate hard copy of the CRB disclosure document sent P&C through the post by TMG. This disclosure is identical to that received by the applicant with the exception of any soft information.

9.3.3 CRB disclosures are held in a fireproof safe. This safe is located in office premises and the building is alarmed with a direct response/police attendance service in place.

9.4 Updates/expansion of data

9.4.1 Additional information will only usually be acquired if further investigation is deemed necessary by the Case Management Group (CMG). This information will usually be solicited by post. It is normal practice to do this by a secure method of delivery, **not** recorded delivery. The CMG has a standard letter to send in the first instance and the follow up methods will depend on the nature of the disclosure and the response or otherwise of the individual.

9.5 Archiving of Data

9.5.1 Data relating to Case Management decisions and CRB disclosure information will be retained **as long as that person remains in Association membership plus 3 years**, where it is possible to do this without compromising any individual's confidentiality; otherwise the information will be held indefinitely.

9.5.2 Hard copy file notes are archived in paper wallets and held in a fireproof safe. This safe is located in office premises and the building is alarmed with a direct response/police attendance service in place.

9.5.3 The data identifying the individuals are held on a computer. This computer does not have internet access nor is it part of a network. The data is password protected.

9.5.4 Both the case notes and computer data will be archived until **3 years after the individual has left the BAB**.

9.6 Deletion / disposal of data

- 9.6.1 Once the CMG has made a decision on a CRB disclosure then the disclosure itself is shredded. TMG are advised of this on the day of disposal.
- 9.6.2 Once the archive period has elapsed then all documents will be shredded.

9.7 Release of information to the individual

- 9.7.1 CRB information should not be held at Association level other than the unique application reference number and date. This is held as proof that the CRB check has been made and when.
- 9.7.2 All requests for visibility of CRB disclosure information should be referred back to the Criminal Records Bureau as it is technically their information to release. Should legal representation be made of the BAB for disclosure release, the BAB Lead CPO will seek advice from CPSU and/or other relevant legal bodies as to the way forward.

9.8 Release of information to third parties

- 9.8.1 It is the BAB's understanding that the welfare of children should over-ride all other considerations, providing that any disclosure of information is reasonable, relevant and proportional.
- 9.8.2 The BAB Lead CPO will as part of his/her work routinely release details of CRB disclosures in order to facilitate the work of the CMG. However, there will be no identifying information released. Members of the CMG operate according to a Code of Confidentiality and will destroy all emails and documentation once a decision has been taken.
- 9.8.3 Any other disclosures to third parties will be undertaken in consultation with the appropriate organisations (e.g. CPSU, NSPCC). However the welfare of the child will always be the priority in the absence of such advice being available.
- 9.8.4 Where possible, information will be disclosed to third parties using postal services such as Recorded Delivery or Special Delivery.

10 Child Protection – Incident Management

10.1 Responsibilities

10.1.1 The responsibility of how the data is handled during the management of a Child Protection Incident is managed by the BAB Lead Child Protection Officer (BAB Lead CPO).

10.2 Introduction

10.2.1 The BAB has a Child Protection Incident Management Policy.

10.3 Inception/acquiring of data

10.3.1 Details of incidents will usually be reported to the BAB by an individual Association CPO or CWO using the CP Policy template.

10.3.2 However it is possible that incidents will be recorded by the Lead CPO, for example, in instances of 'whistle-blowing'.

10.3.3 Copies of any relevant information (eg Instructor course history etc) will be kept within the file. The file will not reference data held externally. In this way, there is no risk of the data being deleted in a different area.

10.4 Updates/Expansion of data

10.4.1 Additional information is acquired on a case-by-case basis. Sometimes it will be necessary to meet with individuals and if so a meeting report will be produced which will be added to the case notes.

10.5 Archiving of Data

10.5.1 Case notes will be retained as hard copy **until the youngest person involved (either directly or indirectly) reaches the age of 21**. If this does not apply then the case notes will be held until such time as the person/s involved are no longer members of the BAB. If none of the above applies, then the data shall be held for a period of **3 years after the file is 'closed'**.

10.6 Deletion / disposal of data

10.6.1 Once the archive period has elapsed as defined above then all documents will be shredded.

10.7 Release of information to the individual

10.7.1 Requests for access to BAB case notes should be made in writing to the BAB Secretary with the appropriate fees as detailed elsewhere in this policy document.

10.7.2 The BAB Lead CPO reserves the right to take advice from the CPSU and/or other relevant legal bodies concerning what information may and may not be released on a case-by-case basis.

10.7.3 Case notes may also be held at Association level and requests for access to this data should be made in accordance with the Association's data handling guidelines.

10.8 Release of information to third parties

10.8.1 It is the BAB's understanding that the welfare of children should over-ride all other considerations, providing that any disclosure of information is reasonable, relevant and proportional.

10.8.2 Any other disclosures to third parties will be undertaken in consultation with the appropriate organisations (e.g. CPSU, NSPCC). However the welfare of the child will always be the priority in the absence of such advice being available.

10.8.3 Where possible, information will be disclosed to third parties using postal services such as Recorded Delivery or Special Delivery.

11 Child Protection – Disciplinary Issues

11.1 Responsibilities

- 11.1.1 The responsibility of how the data is handled during the management of a Child Protection Disciplinary Panel hearing is managed by the Chairman of the BAB in the capacity of President of the Disciplinary Panel.
- 11.1.2 Should the Chairman be under scrutiny, another Executive Board Officer will take this role.

11.2 Introduction

- 11.2.1 The BAB has a Child Protection Disciplinary Panel (CPDP) Management Policy.

11.3 Inception

- 11.3.1 Details of CP decisions made by the BAB CMG which are not accepted by an Association or the individual concerned will be reported to the CPDP (to the President of the Panel) by the Lead CPO. This will normally consist of telephone calls or email, however, no details will be transmitted through either medium.
- 11.3.2 The President of the Panel will then call a meeting of the CPDP to adjudicate on the decision of the CMG and the contestation of that ruling.
- 11.3.3 The case file will be made available to the meeting and added to by the Lead CPO as necessary.

11.4 Update / Expansion

- 11.4.1 Additional information may be acquired on a case-by-case basis. Sometimes it may be necessary to meet with individuals and if so a meeting report will be produced which will be added to the case notes. This report must be signed off by the interviewer and interviewee and any witnesses present and consequently cannot be taken in shorthand.
- 11.4.2 Both the handwritten notes and the ensuing report will be forwarded to the Lead CPO by hand or recorded/special delivery for inclusion into the case file.

11.5 Archive

- 11.5.1 As the data is now part of the CMG file, archive is handled in accordance with section 10.5 of this document.

11.6 Deletion

- 11.6.1 As the data is now part of the CMG file, deletion is handled in accordance with section 10.6 of this document.

11.7 Release of information to the individual or to third parties

- 11.7.1 As the data is now part of the CMG file, the release of information to the individual or to third parties is covered by sections 10.7 and 10.8 of this document.

12 Data Protection Information

12.1 Responsibilities

12.1.1 The control of Data Protection information is managed by the BAB Data Protection Officer (BAB DPO).

12.1.2 All breach incidents are also managed by the BAB DPO.

12.2 Introduction

12.2.1 The BAB DPO manages a list of current Association Data Protection Officers (ADPO). This includes personal information: address and contact phone numbers.

12.3 Inception

12.3.1 All Associations complete two forms. One details the personal contact details of the current ADPO. The second indicates that either the Association is registered with the ICO or will abide by the guidelines issued by the BAB DPO. **It is a requirement for all Associations to submit this information and keep it accurate otherwise they fail to meet the membership requirements of the BAB.**

12.3.2 The information is transposed to a database, held by the BAB DPO. In addition, the paper copies are kept locked away securely.

12.4 Update / Expansion

12.4.1 The data is audited every **2 years** for accuracy.

12.4.2 When updated forms are received, the database is updated and the original forms shredded.

12.5 Archive / Deletion

12.5.1 There is no requirement for the BAB to hold archive information of “past” ADPO's.

12.6 Additional Information

12.6.1 Should an Association cease to be a member of the BAB, the ADPO information is destroyed with **1 month** of the announcement being made (both electronically and physically).

13 Other Disciplinary Issue - Management

13.1 Responsibilities

- 13.1.1 The Disciplinary Sub-committee is responsible for the management of the data handled there-in.
- 13.1.2 It must be re-stated that Child Protection issues are handled in a separate section.

13.2 Inception /Update / Expansion

- 13.2.1 As part of any disciplinary procedure, the Disciplinary Sub-committee will be briefed by the BAB Chairman as to their responsibilities.
- 13.2.2 Any documentation collated during the investigation will be held securely by the chairman of the Disciplinary Sub-committee.
- 13.2.3 Where references are made to external documentation, copies of that documentation will be included in the disciplinary file.

13.3 Archive / Deletion

- 13.3.1 Once the investigation is completed, the file will be sealed and archived by the BAB Secretary.
- 13.3.2 The file will be kept for the statutory minimum length of time (generally **3 years** but could be longer under certain situations).
- 13.3.3 Subsequent to the file exceeding the required length of time, the file will be shredded.

14 General Requests - Access to Data

14.1 Responsibilities

14.1.1 All requests for access to data are managed via the BAB Secretary.

14.2 Request for Access

14.2.1 It must be remembered that the membership of the BAB consists of the Aikido Associations themselves and not their members. An Association can request copies of all their data.

14.2.2 However, as personal Information is also held, any **member** can make request in the same manner as an Association. This means that, for this section alone, Members and members are treated the same.

14.2.3 Any Association may have sight of their data. All that is required is the following:

- A letter sent to the BAB secretary, requesting their information,
- A cheque for £150 for administration purposes made out to the British Aikido Board.

14.2.4 It is best practice that if this is a formal request (eg for legal purposes), the letter requesting the information should be sent by registered delivery. This is in the unlikely case that the letter is lost in the post.

14.2.5 The BAB Secretary will liaise with the BAB DPO in order to confirm that the request for information is legitimate. If not, the cheque will be returned and the letter archived for **3 years**.

14.2.6 Should the request be legitimate, the BAB secretary will contact all BAB officers to ensure that any information matching the request and controlled by them is copied and returned to the BAB secretary within **20 working days**.

14.2.7 The BAB is duty bound to supply this information within **30 working days** of receipt of this request.

14.2.8 Should the information requested include CRB or Child Protection information, there may be an unspecified additional delay while legal questions are resolved.

15 Breach and Notification Process

15.1 Responsibilities

- 15.1.1 Should a Data Protection breach be identified, (including loss or theft of computer equipment holding information), the BAB DPO must be informed with utmost urgency.
- 15.1.2 The BAB DPO will instigate the process of Detection and Investigation of Security Breaches (defined below) in direct discussion with the ICO.

15.2 Detection and Investigation of Security Breaches

15.2.1 Notification

- 15.2.1.1 Once the BAB DPO has identified the nature and quantity of the data lost and the extent of the breach, the ICO will be contacted.
- 15.2.1.2 Law enforcement will be informed at the earliest possible opportunity should any criminal act be suspected and if directed by the ICO.
- 15.2.1.3 All potentially affected people will be notified in writing of the situation as and when deemed appropriate by the ICO.

15.2.2 Lockdown

- 15.2.2.1 Should an individual involved in the loss of the data hold other data, that information will be secured.

15.2.3 Incident Management

- 15.2.3.1 The Incident will be managed by the BAB DPO in conjunction with the ICO and law enforcement as necessary.
- 15.2.3.2 The BAB DPO will complete a dossier detailing all aspects of the breach. The lifecycle of the dossier will be indefinite.
- 15.2.3.3 In addition, the BAB DPO will write a report of the incident for publication to its members. This report will exclude personal information and will be cleared by the ICO prior to publication.

This page is intentionally blank