CONFIDENTIALITY POLICY AND PROCEDURE

Policy Statement

BAS will adhere to principles of honesty, openness and transparency in all its operational and organisational activities. There are times however when some information held by the organisation has to be regarded as confidential to the organisation. In such circumstances all Employees are required to maintain strict confidentiality regarding such information. As much information is nowadays held on computer systems, this policy is written in terms of the confidentiality of information using a computer. Its principles apply to all information.

This section focuses on confidentiality in relation to clients and follows with confidentiality requirements relevant to the internal operation of, and the Employees employed by, the organisation.

BAS encourages Employees, Contractors and Volunteers in the use and development of IT systems and facilities that enhance our operational efficiency. However, the availability of email and the internet can lead to problems ranging from 'email overload' and computer viruses to matters that could cause legal claims against the organisation. You should therefore be fully familiar with this confidentiality policy and BAS' Internet and Email Security Policy – see below.

Confidentiality Policy in relation to clients

Confidentiality Statement - BAS is committed to providing a confidential information and support service to its clients. We believe that principles of confidentiality must be integrated across all aspects of services and management. BAS believes its clients deserve the right to confidentiality to protect their interests and safeguard the organisation's services.

Definition of Confidentiality - BAS understands confidentiality to mean that no information regarding a client shall be given directly or indirectly to anyone outside the organisation, without that client's prior expressed consent to disclose such information.

We recognise that information may be indirectly given out through Employees informally discussing clients. All Employees should ensure that no discussions relating to an individual take place where they can be overheard by a third party. The Board of Trustees will not receive identifying details of individuals, or their case. BAS will not confirm the client's presence in the office base or use of the organisation's services without obtaining the client's consent. BAS is a voluntary organisation working in partnership with local authorities and is required to follow local Child Protection and Vulnerable Adult procedures when abuse is brought to attention.

Statistical Recording - BAS is committed to effective statistical recording of clients to enable the organisation to monitor take-up of service and to identify any policy issues arising. It is the Chief Executive 's responsibility to ensure all statistical records given to third parties, such as to support funding applications, monitoring reports for the local authority shall be produced in anonymous form, so individuals cannot be recognised.

Case records - It is the Chief Executive 's responsibility to ensure all case records in the office are kept securely. This includes notebooks, copies of correspondence, calculation sheets and any other sources of information. All Employees/Volunteers are given guidance on the safe storage of information relating to clients. When Employees work from home, the Employee holds responsibility for maintaining the security of BAS client information.

Expressed consent to give information - It is the responsibility of Employees/Volunteers to ensure that where any action is agreed to be taken by the organisation on behalf of a client, that client must firstly give their consent which should be recorded. BAS Employees/Volunteers are responsible for checking with clients if it is acceptable to call them at home or work in relation to their case. All Employees/Volunteers must ensure they make no reference to BAS when making telephone contact with clients unless the client has agreed to this. Employees/Volunteers are responsible for checking with clients that it is acceptable to write to them at home or work in relation to their case. All details of expressed consent must be recorded.

Safeguarding – vulnerable adults and children – exclusion from confidentiality - Where the safety and welfare of vulnerable adults or children are at risk, their protection takes precedence over the requirement for confidentiality. On occasions where an Employee/Volunteer feels that Safeguarding may be an issue, the following steps must be taken:

- The Employee/Volunteer should make notes of any events/ discussions causing concern as soon as possible.
- The Employee/Volunteer should raise the matter immediately with the Chief Executive .
- The Employee/Volunteer must discuss with the Chief Executive the issues involved in the case. The Chief Executive should take a written note of this discussion.
- The Chief Executive is responsible for making a decision whether or not to contact Social Services about the matter. Once contact is made with Social Services, the Chief Executive will take whatever action is advised by this agency.
- The Chief Executive should brief the Chair on the full facts of the case, ensuring they do not breach confidentiality in doing so.
- A full written report on the case should be made and any action agreed, undertaken. The Chief Executive is responsible for ensuring all activities are actioned.
- If the Chief Executive is not available, any concern should be passed to nominated members of staff or Trustees who will decide whether Social Services should be contacted.

- The case should not be discussed with other members of the Board who may have to resolve any future complaint about the action taken.

Legislative Framework - BAS will monitor this policy to ensure it meets statutory and legal requirements.

Ensuring the effectiveness of the policy - All members of the Board of Trustees will receive a copy of the Confidentiality Policy. Existing and new Employees and Volunteers will be introduced to the Confidentiality Policy via induction and training. The Policy will be reviewed annually and amendments should be proposed and agreed by the Board.

Passwords - Whilst BAS takes all reasonable steps to protect our systems from the external environment, external links make our systems more vulnerable. It is important, therefore, that all Employees ensure that they adhere to our security requirements. Passwords provide the most critical and potentially weakest link in the security chain. Never write your password down or share your password and never let anyone else use your Client ID and password. If you think someone is aware of your password you should change it immediately.

Equipment and Software - At the end of each day you must ensure you sign off from each system. Shut down your machine and switch it off before you leave the office.. In order to comply with the licensing laws regarding software, only software that has been purchased by the organisation and installed by us is recognised as being legal software. Any unlicensed software found will be deleted and disciplinary action may be taken against you, including in serious cases, dismissal.

Personal Use - Private personal use of computers must be kept to a minimum.

Training - If training is required on software, you should contact the Chief Executive who will coordinate the training.

13 INTERNET AND EMAIL SECURITY POLICY

Internet Use - The internet provides opportunities of accessing information and of communicating with others. However, internet access will also expose BAS to a number of new liabilities. Employees' activities on the internet can result in potential liabilities for the organisation. These liabilities could arise in a number of areas, for example:

Defamation - Clients tend to view email in the same light as a telephone call. They also tend to be more indiscreet than if they were sending a letter or memo. This increases the risk of liability for defamatory statements in emails. There is also possible direct liability for BAS as publisher of the message. You should not commit anything to email that you would otherwise not wish to put in writing.

Pornography - There is no legitimate interest in Employees, Contractors or Volunteers accessing or transmitting pornography on the Internet. Contravention of this policy may result in disciplinary action being taken against you and in serious cases dismissal and/or criminal prosecution.

Viruses - All software downloaded from the internet must be subjected to rigorous anti-virus checks.

Copyright infringement - The main risk of copyright infringement applies to downloading files from the internet. Copyright infringement can also occur with email attachments. If in doubt you should seek advice from the Chief Executive .

External communications - External communications published electronically and identified as coming from BAS have the same effect as in a letter or other written document and should be subject to the same controls. Suitable notices and disclaimers should be used where any liability issues are in question. Commercial negotiations should be described as "subject to contract".

Personal communications - should be kept to a minimum.

Code of Conduct for Internet Clients - Internet access is provided for the use of Employees, Contractors and Volunteers in conducting BAS business. While the internet represents a potentially valuable resource, it also exposes the organisation and its Employees to a variety of risks. Therefore, all aspects of our Internet presence must be carefully managed to ensure that our image is properly protected, that its liability is limited, that its internal resources are protected from outsiders, and that internet use by Employees, Contractors and Volunteers is cost-effective and suitable for operational purposes.

As a client of the provided internet access, you must:

- gain access to internet resources only through authorised means;
- represent yourself and the organisation professionally in all your use of the internet;
- use your internet access only for authorised purposes;
- ensure that any non-official use is inconsequential in its use of organisation resources (work time, network resources, computer storage space) and complies in every way with policies for appropriate use;
- use internet access only in ways consistent with our standards of conduct;
- comply with UK law (and the law of other jurisdictions, where appropriate) regarding electronic communications;
- ensure that none of your actions create legal or security risk to BAS, damage the reputation of the organisation, or cause embarrassment to the organisation;
- minimise downloading of files to manage consumption of network resources;
- report known or suspected breaches of security and violations of internet policy to the Chief Executive immediately.

You must not:

- permit access to resources in our internal network to any outside source other than through authorised security procedures;
- participate in non-BAS related news groups;
- transmit proprietary or confidential information via the internet or in any other way, except where approved by the Chief Executive or a Trustee;
- transmit any material which might be considered defamatory of any person, company or other organisation;
- transmit any unlawful material, including material which is discriminatory, blasphemous or obscene, or which may constitute harassment, whether of the recipient or any other person;
- enter into any contract on the Internet or by e-mail without prior authorisation and in accordance with organisational procedures.

Email Use - Use of email by Employees of BAS is permitted and encouraged where such use supports the aims and objectives of the organisation. However, BAS requires that all Employees must ensure that they:

- Do not breach any of BAS policies in their use of email or other means of electronic communication.
- Do not share or transmit confidential information except at the direct and express request of and with the explicit permission of clients.
- Use a password-protected system at all times to ensure the confidentiality of work undertaken on behalf of the organisation.
- Use email in an acceptable way and in accordance with this policy whether accessed from BAS' office premises or remotely, via home-based/personal IT equipment.
- Comply with current legislation.
- Do not create unnecessary risk to the organisation by their misuse of the internet.

Unacceptable behaviour - The following behaviour by an employee is considered unacceptable:

- Use of organisation communications systems to set up personal businesses.
- Forwarding of confidential information to external locations, other than by return to clients.
- Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal.
- Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment.
- Accessing copyrighted information in a way that violates the copyright.

- Breaking into another organisation's system or unauthorised use of a password/mailbox.
- Broadcasting unsolicited personal views on social, political, religious or other matters.
- Transmitting unsolicited commercial or advertising material.
- Undertaking deliberate activities that waste staff effort or networked resources.
- Intentionally introducing any form of computer virus or malware into the corporate network. Employees must never import files, programs or unknown messages onto their systems without ensuring they have first been scanned for viruses

Monitoring - BAS accepts that the use of email is a valuable working tool. However, misuse of this facility can have a negative impact upon the charitable purpose, operational intent and reputation of the organisation.
In addition, all of the organisation's email resources are provided for business purposes. Therefore, the organisation maintains the right to examine any systems and inspect any data recorded in those systems. In order to ensure compliance with this policy, BAS also reserves the right to use monitoring software in order to check upon the use and content of emails. Such monitoring is for legitimate purposes only and will be undertaken in accordance with a procedure agreed with employees.

Sanctions - Where it is believed that an Employee has failed to comply with this policy, they will face the organisation's disciplinary procedure. If the Employee is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the employee's disciplinary record. Email should be regarded in the same light as letters or memos. You should not commit anything to email that you would otherwise not wish to send out in writing. The email system is to be used for communication directly relating to the organisation's activities. Personal use of the system causes a distraction for you as an Employee, Contractor or Volunteer and therefore personal use should be kept to a minimum (and in any event outside of your working hours). You should be aware that email systems can be monitored and that system abuse will be reported to the Chief Executive . BAS will not tolerate any email message that might amount to harassment or bullying of an Employee or Volunteer, or which might bring our name into disrepute. These will be dealt with under the organisation's disciplinary procedures.