Keele University Students' Union

CONFIDENTIALITY POLICY

ADVICE & SUPPORT AT KEELE IS COMMITTED TO PROVIDING A CONFIDENTIAL ADVICE SERVICE TO ITS USERS.

Advice and Support at Keele, (ASK) provides free, confidential, independent, impartial, non-judgmental advice, information and representation to Keele students[1].

ASK believes that principles of confidentiality must be integrated across all aspects of services and management. ASK believes its users deserve the right to confidentiality to protect their interests and safeguard ASK's services.

The Confidentiality Policy and Procedure is contained in the first half of this handbook. The second section details some of the issues we need to be aware of in our day-to-day working practices and provides information on the legal framework we are working with.

ASK delivers a confidential service - nothing you tell us will be shared with any other organisations or individual without your express permission. (See 'Breaches of Confidentiality').

ASK understands confidentiality to mean that no information regarding a service user shall be given directly or indirectly to any third party who is external to the ASK team, Deputy Chief Executive Officer (Membership) and KeeleSU Chief Executive Officer (CEO) without that service user's prior expressed consent to disclose such information.

ASK recognises that all users should be able to access ASK's services in confidence and that no other person should ever know that they have used ASK.

Service users need to be aware that if we suspect, or have evidence of child abuse, we will pass that information to Children and Family Social Work teams and / or the police.

ASK recognises the risk that information may be indirectly given out through staff informally discussing cases. All staff should ensure that no discussions relating to an individual user of ASK can take place outside of ASK. The Senior Leadership Team will not receive details of individual users or their case. ASK recognises that users need to feel secure in using the ASK's services in a confidential manner. ASK will ensure all users are afforded confidential interview space (if it is required) and will ensure blinds, radios and other mechanisms are used to ensure no breach of confidentiality can occur inadvertently. Cases will not be discussed in public places even when names are not mentioned. ASK will not confirm the user's presence in the centre or use of the centre without obtaining the user's consent.

[1] See the Code of Practice for current definition of 'student'.

ASK is committed to effective statistical recording of service users to enable us to monitor take-up of service, to identify any policy issues arising from advice services, and to inform proactive campaign work. It is the ASK Manager's responsibility to ensure all statistical records given to third parties, such as to union and university committees, shall be produced in an anonymous form, so individuals cannot be recognised. It is the ASK Manager's responsibility to ensure that any Good News Reports are produced in an anonymous form ensuring individuals cannot be recognised.

It is the ASK Manager's responsibility to ensure all on going case records are kept secure. All case records must be secured at the end of each working day. All information relating to service users secured, this includes note books, copies of correspondence, calculation sheets and any other sources of information.

It is the ASK Manager's responsibility to ensure that Independent File Review sheets are secured.

It is the responsibility of ASK Advisers to ensure that where any action is agreed to be taken by ASK on behalf of a client, that client must firstly sign an authorisation form or email ASK with authorisation from their Keele email account. This should be recorded on the client's file.

ASK workers are responsible for checking with clients if it is acceptable to call them at home or work in relation to their case. All staff must ensure they make no reference to ASK when making telephone contact with clients, although if a message is taken and a name is required, we will leave a first name only. When writing to clients, envelopes should not reveal the source of the letter. ASK workers 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 on the case file.

Breaches of Confidentiality: ASK recognises that occasions may arise where individual workers feel they need to breach confidentiality. ASK recognises, however, that any breach of confidentiality may damage the reputation of ASK and therefore has to be treated with the most serious of approaches. On occasions where a worker feels confidentiality should be breached the following steps must be taken:

1. The worker should raise the matter immediately with the ASK Manager.
2. The worker must discuss with the ASK Manager the issues involved in the case and explain why they feel confidentiality should be breached and what would be achieved by breaching confidentiality. The ASK Manager should take a written note of this discussion.
3. The ASK Manager is responsible for discussing with the worker what options are available in each set of circumstances.

4. The Deputy Chief Executive Officer (Membership) is responsible for making a decision on whether confidentiality should be breached. If the Deputy Chief Executive Officer (Membership) is unavailable the decision should be made by the ASK Manager. If neither the Deputy Chief Executive Officer (Membership) nor ASK Manager is available, another senior person should make the decision.

   It may be appropriate to discuss the case with a specialist service for guidance. **Care should be taken to make sure confidentiality is not breached at this stage.** Examples of a specialist service are the NSPCC for child protection issues, Women's Aid for domestic violence or Keele Mental Health & Wellbeing team for mental health issues.

If confidentiality is to be breached then they should take the following steps:

A. A full written report on the case should be made and any action agreed undertaken. The Deputy Chief Executive Officer (Membership) is responsible for ensuring all activities are actioned.

B. In no circumstances should any breach of confidentiality be discussed with the Union Development & Democracy (UDD) Officer. This is to ensure that any future complaints or investigations arising from a breach in confidentiality can be carried out in an independent manner.

ASK will monitor this policy to ensure it meets statutory and legal requirements. Please see Legal Issues section.

All of the Management Committee members will be made aware of the confidentiality policy and its contents. Existing and new workers will be introduced to the confidentiality policy during induction and ongoing training. ASK volunteers will also be asked to agree to this policy.

Person responsible for review: ASK Manager

ASK AND CONFIDENTIALITY

1 WHO IS COVERED BY THE POLICY?

1.1 The service user should be able to assume that anything they disclose to a worker in ASK will remain within ASK, subject to statutory restrictions.

1.2 Confidentiality rests with ASK, not individual workers, so it is perfectly acceptable for all workers in ASK to have access to case records, take part in discussions relating to the service user's enquiry. Administrative workers will also have access to service user details so they must also receive details of the policy and understand the implications of its operation. The ASK Manager will hold signed copies of the policy. See para 2.4.4.

1.3 The Senior Leadership Team are not covered by the confidentiality policy except the Deputy Chief Executive Officer (Membership) and Chief Executive Officer – and do not have access to case records nor be made aware that an individual has consulted ASK. Clearly, the Senior Leadership Team should be aware of the policy.

1.4 Confidentiality rests with the service user. There will be some instances where other people may act on the service user's behalf – collecting and bringing in information for example. We have a responsibility to the service user to ensure that they have given this person their permission – again, in writing is best.

1.5 It is important that we do not disclose that the service user has visited ASK or is currently in ASK premises unless we have their consent to reveal the information. So partners, children, relatives enquiring if the individual has visited /is visiting should be made aware of this Confidentiality Policy. We can check with the service user if it is all right to confirm their presence. The same approach applies to social services, probation officers, the police, the University – only talk with them about the service user, even to the extent of confirming they visit the centre, with the user's permission.

1.6 Try to avoid working through a third party such as a relative or a social worker. On a practical note, information can be missed or get confused.

2 WORKING WITHIN A CONFIDENTIAL SETTING

2.1 It is important that our organisational procedures and systems guard against breaches of confidentiality.

2.2 INCOMING/OUTGOING POST

2.2.1 Ensure all workers who have contact with post are aware of the confidentiality policy. Always check with the service user that it is all right to send letters to their

home – this might not be the case in a relationship break-up. The same applies with regards to telephone calls – it will not always be the service user that answers the phone – do not give details to other people. Do not leave messages (except on individual voice mail) unless someone has checked with the service user first.

2.3 CONTACT WITH A THIRD PARTY/REFERRAL SERVICE

2.3.1 Whoever we contact on behalf of a service user, or about a service user, we need to ensure we have the service user's consent. There are benefits in obtaining written consent – many agencies will want to see the user's written consent before they reveal details e.g. banks, some Local Authority departments. ASK has authorisation slips that the service user can complete.

2.3.2 When referring on, ensure that written permission to pass on a copy of the case record to a solicitor or 2nd tier agency is obtained. Equally, when a solicitor contacts ASK requesting the service user's case records, ensure you ask for the service user's request in writing.

2.3.3 Remember: the case records are equally the property of ASK –always keep a copy of the case record at ASK even when the case is completed.

2.4 STORING RECORDS

2.4.1 Notebooks used by workers will need to be shredded or disposed of carefully.

2.4.2 Case records, Checking Forms and Independent File Review Forms should be stored in lockable cabinets/drawers or rooms not accessible by the public.

2.4.3 It is good practice to keep records for 7 years. When dormant, paper files / cases can be boxed alphabetically in year groups and kept in a locked cupboard/room. After 7 years since the last contact they must be shredded/incinerated.

2.4.4 Student Case Manager is hosted in the UK in a professional 3rd party datacentre which is certified to ISO27001

· All MSL staff with direct access to the data are permanent employees who operate a formal Information Security Management System and receive regular training on the maintenance of data security

· The case management service is governed by a formal licence and services agreement between Keele SU and MSL which acknowledges the roles of MSL as data processor and the customer as data controller, and maintains the obligation on MSL to comply with the provisions of the Data Protection Act 2018.

· Information about clients is only processed by MSL for the purposes of managing the client's case by the provision of advice services and for anonymised management reporting and audit

· MSL does not disclose personal information to third parties for any purposes, under any circumstances except as required by law.

2.5 DATA COLLECTION

2.5.1 It is essential to gather statistical data; this must not identify individuals. "Good news" and 'evidence' reporting data is collected; this must not identify individuals.

2.6 PRIVACY

2.6.1 We should, as far as we are practically able, ensure we achieve privacy in the waiting areas, general office and interview rooms. Service users should feel comfortable.

2.6.2 Service users should be made aware that interview rooms are available should they want to use them. Use blinds to minimise visibility if necessary. Care needs to be taken that others cannot hear conversations or telephone calls. Use offices for telephone calls. Use radio/CD's to help block the noise. One to one sessions are appropriate in the majority of cases but ASK sometimes operates open sessions. If the service user is happy with having their question answered in an open setting, this is fine - as long as it is their choice.

2.7 USE OF E-MAIL.

2.7.1 Clients contacting ASK using electronic mail are to be informed of the following. *"ASK is happy to advise students and staff using electronic mail. However, ASK cannot ensure confidentiality using this medium in the same way as contact through interviews, telephone or letter. Therefore, we recommend that if you wish to contact us using electronic mail please treat it as if using a post-card, if you need to divulge sensitive information you may prefer to do so in a different way. If you do contact us for advice using electronic mail we will assume you are happy for us to respond in this way."*

2.8 Section removed.

2.9 Social Policy / Evidence sheets

2.9.1 Evidence sheets are collected to monitor patterns or trends. Such reports should safeguard against disclosing identifiable service user details-unless they expressly agree. ASK is committed to effective statistical recording of service users to enable ASK to monitor the take up of service and identify any policy issues arising about or from advice services. It is the ASK Manager's responsibility to ensure all

statistical records given to third parties are produced safeguarding against disclosing identifiable user details – unless they expressly agree.

2.10 Outreach and storing records at home.

2.10.1 In the case of ASK Advisers offering an outreach service, arrangements will be made to ensure that sessions are conducted to protect confidentiality, though the level of protection may be limited due to the nature of the facilities at the outreach site. Records will be kept with the outreach worker and time will be allocated for the Adviser to return to ASK to store records appropriately.

2.10.2 There may be occasions when following an outreach session or an Adviser has been working from home that the Adviser is not able to return to store the files in locked cabinets within ASK. If this happens the Advisers will ensure that records stored at home are kept secure and family or friends have no access to them, records are to be returned at the earliest opportunity, no later than the next working day.

3 LEGAL ISSUES

There is a legal framework for confidentiality. We need to be aware of these issues in order to make an informed decision.

3.1 DISCLOSURE OF CRIME

3.1.1 There may be instances when ASK users confide that they have committed/are about to commit a crime. In English Law there is no duty to disclose a criminal offence so being aware of the crime is not assisting in that crime.

3.1.2 There are important exceptions:

The Social Security Administration (Fraud) Act 1997.

The Terrorism Act 2000.

3.1.3 Please also see the 'Withdrawal of Service Statement'.

3.1.4 It is an offence to aid, abet, counsel or procure the commission of an offence. It is therefore important that the adviser makes sure that s/he does not give, or in any way can be seen to be giving, encouragement or assistance in any way.

3.1.5 Do not destroy the relationship you are developing with the user by alarming them but ensure that if you have concerns about the information the user is disclosing, you tell them:

- that what they are saying/about to say could break the law;

- that you can assure them of confidentiality but need to warn them not to give any further details and they should seek advice from a solicitor;

- you may be later summonsed as a witness.

3.2 POLICE ATTENDING ASK

3.2.1 The police may approach ASK to gather information about a service user. If you have advance warning of the visit adopt the following procedure:

* inform the police that you operate a confidentiality policy and offer to go through its contents.

* ensure all workers and users are aware that the police will be attending ASK – thereby giving users the option to leave.

* the police officers should not be allowed to enter any room where records are kept (i.e. Resource Room & Deputy Chief Executive Officer's (Membership) Office).

3.3 PROVIDING INFORMATION TO THE POLICE

3.3.1 If you feel under pressure to reveal information to the police e.g. you are threatened with arrest, the following is the legal position:

3.3.2 The police have powers under the Police and Criminal Evidence Act 1984 (PACE). This provides general powers to police officers, lawfully in any premises, to seize anything that they reasonably believe is evidence in relation to an offence under investigation, which might otherwise be concealed, lost, altered or destroyed. Preventing access to a room where records are kept forestalls the use of these powers. It is important to note that PACE only allows access to materials which would have been available to the police before 1986 and personal, confidential case records were not included.

3.3.3 The police can summons a worker as a witness. Failure to attend may result in the Court issuing a warrant to arrest and bring the witness before the Court. Failure to do so could result in a fine or committal to prison.

3.3.4 ASK can negotiate with the police or when attending the magistrates court and explain case records are confidential. ASK should also inform the service user that the summons has been received and the penalties that may be levied. Workers should not discuss the evidence to be given with the service user.

3.4 CRIMES COMMITTED IN ADVICE & SUPPORT AT KEELE

3.4.1 If the police are called following a break-in, care should be taken to ensure that cases are in locked cabinets, though evidence must not be disturbed!

3.4.2 If case records have been stolen, the police should be told that they are confidential and should be returned, unread, if possible. If you need to call the police because of a crime committed in ASK e.g. theft from the waiting room, following the steps outlined in the section on "Police attending ASK".

3.5 CHILD ABUSE

3.5.1 Some crimes may receive higher media profile and others can provoke a reaction from workers. Child abuse is one such issue. You may receive an enquiry from a person who tells you they are the abuser or your client may be the victim of abuse (the Children Act 1989[2] ensures that children can make enquiries independent of their parents so long as they have enough understanding and intelligence to make up their minds).

3.5.2 The legal position is that whilst some agencies, notably the police, have a statutory duty to report suspicions or evidence of child abuse to social service departments, this duty does not apply to voluntary services. Whilst local authorities have a mandatory duty to investigate if they are informed a child may be at risk, there are no specific mandatory child abuse reporting laws in the UK that require professionals to report their suspicions to the authorities[3]. We must make our position clear in that service users need to be aware that if we suspect or they have evidence of child abuse **we will pass that information to Children and Family Social Work Teams** and hence this would breach client confidentiality.

3.5.3 The enquirer should be referred onto a professional agency that have the resources and skills to counsel and support them.

3.5.4. Please see the University 'Policy for the Safeguarding of Children, Young People and Vulnerable Adults'.

3.6 DATA PROTECTION ACT 2018

3.6.1 All information is kept in accordance with the Data Protection Act 2018. We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect.

3.6.2The Data Protection Act 2018 brought the UK in line with the European directive on data protection (GDPR). The legislation applies to manual files as well as

2 The Children Act 2004 does not replace or even amend much of the Children Act 1989. Instead it sets out the process for integrating services to children. Child Protection Factsheet, NSPCC October 2011 page 5
3 An introduction to child protection legislation in the UK. Child Protection Factsheet, NSPCC October 2011 page 3.

those held on computer. In relation to confidentiality it provides a useful point to think about – under the legislation the people we hold information about have to be given certain information and have the right to object to what we do with it in some circumstances. This is not new and accords with good practice – it means that we should take care to record only relevant objective information and avoid judgmental remarks and opinion.

3.6.2 See also the Office Manual on case recording and storage.

3.7 FRAUD ACT

3.7.1 The Social Security Administration (Fraud) Act 1997 came into effect on 1st July 1997.

3.7.2 Under the Fraud Act advisers must not knowingly assist in any way with a fraudulent claim. This legislation does not impose a blanket obligation on an adviser or any third party to inform a benefit authority of someone s/he knows to be defrauding it in order to avoid the risk of prosecution. However, ASK advisers should point out to all clients claiming benefits or connected to someone who is claiming benefits, that they are obliged to inform a benefit authority of a change of circumstances and explain the consequences of failing to do so. Advisers should not knowingly assist, in any way, with a fraudulent claim. This has led centres to consider their actions if a user admits to making a fraudulent claim. As a service we can choose to take the same approach as that advised in the section on committing a crime –we are not under an obligation to pass details to the Benefit Agency – and should not, as this would breach confidentiality.

3.7.3 You should follow procedure:

* Explain the legal implications and possible consequences. Record that you have passed on this information.

* Make it clear that the user has a duty to disclose their change of circumstances.

* If the person wishes to continue to use ASK's services but is unwilling to give notification of their change in circumstance, you should consult the Deputy Chief Executive Officer (Membership) to consider ceasing to advise or assist the user with the claim. This will not stop you advising the user on benefits they are able to claim or other issues.

3.7a BRIBERY ACT 2010

3.7a1 "The act creates three main offences:

bribing a person to induce or reward them to perform a relevant function improperly

requesting, accepting or receiving a bribe as a reward for performing a relevant function improperly
using a bribe to influence a foreign official to gain a business advantage.

A relevant function can be an activity associated with the private or public sector provided that the function should be carried out in either good faith, impartially or that the person performing it is in a position of trust".

"A person commits an offence if, directly or indirectly, they request, agree to or accept a bribe:

intending that a relevant function should be performed improperly, either by them or by a third party
when to do so, in itself, would be improper performance of a relevant function
as a reward for carrying out a relevant function improperly, or
in anticipation or consequence that they (or someone else on their behalf) will perform a relevant function improperly"[4]

"Improper performance means performance which amounts to breach of an expectation that a person will act in good faith, impartially, or in accordance with a position of trust. The offence applies to bribery relating to any function of a public nature, connected with a business, performed in the course of a person's employment or performed on behalf of a company or another body of persons. Therefore, bribery in both the public and private sectors is covered"[5].

See also ASK's Gift Policy.

3.8 RISK OF HARM

3.8.1 A worker may be alerted to the possibility that a user may harm themselves or others. This should be discussed with colleagues and options such as a referral to other more appropriate agencies considered. Remember, only contact bodies such as social workers or doctors with the user's consent.

3.8.2 In the case of a service user exhibiting threatening behaviour to other users or staff and if the member of staff believes the threat to be serious the police/ambulance service should be called. If an individual is in danger they have a right to be informed. Do not put others in danger.

3.8.3 Where a member of the ASK team is subject to threatening, violent or abusive behaviour by the user they will be asked to leave ASK, or stop contacting ASK, as appropriate. If a service user is ejected from ASK and security has to be called this

4 From The Law Society's Practice Note on the Bribery Act 2010 http://www.lawsociety.org.uk/support-services/advice/practice-notes/bribery-act-2010/5 Ministry of Justice The Bribery Act Guidance 2010 page 10

will require a breach of confidentiality. See also ASK Withdrawal of Service Statement.

3.9 CONFLICT OF INTERESTS

3.9.1 A conflict of interest arises where ASK can no longer give independent and impartial advice to a client for a particular reason, or where we are seen as not able to give independent and impartial advice.

3.9.2 To be able to advertise our service as impartial there must not be any factor influencing the advice we give other than the clients' best interests. Neither the adviser, nor the organisation should have any significant personal interest in the outcome of the inquiry or case.

3.9.3 We must be able to spot conflicts of interest quickly; the computerisation of case recording makes this easier. However, it is not always easy to identify e.g. a client may have changed their name, or address, the conflict may arise through a relative/third party. Sometimes conflicts are identified through chance conversations.

3.9.4 The most common situations for conflicts to occur are:

- Landlord and tenant (we cannot advice landlords, except where it is in the tenants interest to do so
- Issues arising out of a relationship breakdown
- Harassment
- Plagiarism / Collusion
- Neighbour disputes in halls / off campus accommodation
- We cannot give advice to someone involved in a dispute with the Students' Union, Students' Union staff or services, on that issue, however we can provide help to that individual on other unrelated matters
  Note: It is not a conflict of interests merely to give information (e.g. to explain the University regulations) to both parties in a dispute, however if both parties ASK for representation a conflict will arise, see 3.9.6 onwards.

This list is not exhaustive.

3.9.5 How to identify a conflict of interest:
If the nature of the inquiry means that a conflict is possible:

- Check a name with current records – the central record of clients should be consulted to look for obvious duplications of names and addresses if a conflict of interests is suspected.
- Run electronic check.

- Assess the nature of the inquiry and run a check on other, appropriate information, in order to identify a conflict of interest.
- Check if the two parties are in dispute, if they are, see 3.9.6 onwards. If not, the case should be carefully monitored. ASK Manager should be informed of the case. If both parties subsequently differ and a dispute occurs, the ASK Manager has discretion to deal with the matter appropriately.

3.9.6a Where a conflict or a potential conflict of interest has been identified, *and the two parties are in dispute*, ASK will offer advice, information and representation to the first person accessing the service for help about the specific issue in question. Whilst the subsequent person / people will be unable to access the service regarding that issue, ASK will continue to provide advice and assistance on any other matters. Where other parties approach us and we can't help, due to a conflict of interest, we will signpost them to appropriate alternative services, this may be a Sabbatical Officer who is an elected student representative. We ask clients to observe our Code of Practice.

3.9.6.b This paragraph covers the specific issue of **collusion**. As there are no similar services for students to utilise, ASK has an exception to the conflict of interests policy. Please also see the supplementary flowchart to assist advisers with the process. Clients will be informed of the process verbally and in writing.

In the event of a potential conflict of interest between clients in a collusion case, ASK can still advise both parties, provided that:

· different advisers (with different supervisors) deal with different clients and never discuss their clients with each other and

· both clients are told that the other party is being advised by ASK, understand what the arrangements are, and agree to them. This means that for this purpose alone, the duty of confidentiality does not apply

· ASK has a conflict of interest policy which includes how ASK would deal with this eventuality

In cases of multiple parties, we will judge each case, and try to offer impartial assistance to all involved, however, if at any time our impartiality is compromised, we reserve the right to withdraw help to all parties involved.

3.9.7 Confidentiality will need to be breached when ASK identifies a conflict of interest, as that necessitates ASK informing one party that it cannot act on their behalf. By its very nature, this will draw attention to the fact that ASK is acting for the other party. This should be the only information that is disclosed.

3.9.7a In the case of 02

3.9.8 The Adviser should explain the Conflict of Interest policy, give the client a leaflet about the policy and direct the service user to another agency for help – see the policy on Signposting and Referral.

3.9.9 If ASK has been advising both parties the ASK Manager should be informed. Potentially, both parties could be referred to another agency for assistance – see the policy on Signposting and Referral.

If this is not possible:

3.9.10 Both parties should be informed that a conflict of interest has been identified and that if the case goes further e.g. to a hearing or to court the ASK will cease to act for both parties and that if this is likely the adviser should consider referral at the earliest opportunity. A leaflet explaining the situation 'Conflict of Interests' will be given to the client, where available.

3.9.11 If someone is involved in a dispute with the Students' Union ASK cannot advise that person on that dispute, but can advise on any other matter.

The nature of conflict of interests is that it cannot always be identified as a conflict or potential conflict; issues will be dealt with in accordance with the above guidance and on a case by case basis, the policy being updated on a regular basis.

3.10 Section removed.

3.11 TERRORISM ACT 2000

3.11.1 TERRORISM ACT 2000 (Which replaces the Prevention of Terrorism (Temporary Provisions) Act 1989). The Act places an obligation on the Adviser, as a citizen, to pass on information about planned or actual terrorist offences. Failure to do so is a criminal offence under s.19 of the Act, punishable, on conviction, by a fine or a prison sentence of up to 14 years. It is also an offence under s.39 for an Adviser to inform the service user, or any other person, that information has been passed to the authorities, where such a disclosure is likely to prejudice any investigation. The penalty for the latter offence is a fine and/or a prison sentence of up to five years on conviction. (In these circumstances Advisers must inform the Deputy Chief Executive Officer (Membership) that information has been passed onto the authorities. The ead of Membership Services must inform the Chief Executive Officer when they or any Advisers have had to inform the authorities under this Act.

3.11.2 The definition of terrorism is deliberately vague. Terrorism means the use or threat of action designed to influence the government, or intimidate the public, 'for the purpose of advancing a political, religious or ideological cause'. Such action will include serious violence against a person, serious damage to property, a danger to life, a serious risk to the health or safety of the public, or to electronic systems. The remit of the Act refers to international terrorism, rather than to actions solely occurring within the UK.

3.11.3 Advisers should be aware that if they learn about the terrorism 'in the course of a trade, profession, business or employment' then they could claim a reasonable excuse for not disclosing where:

- he or she is in employment.
- the employer has established a procedure for the making of such disclosures.
- the disclosure followed this procedure.

Guidance on this is not readily available. Staff should be able to make a 'protected disclosure' to the Deputy Chief Executive Officer (Membership) and under the protection of the Public Interest Disclosure Act 1998, as provided for under s.43 of the Employment Rights Act 1996.

Please sign to say that you have received, read, understand and agree to comply with ASK's Confidentiality Policy:

Name:_____

Signature:_____

Date:_____

Index