

Keele University Student' Union Independent Advice Unit



CONFIDENTIALITY HANDBOOK

2011

THE INDEPENDENT ADVICE UNIT IS COMMITTED TO PROVIDING A CONFIDENTIAL ADVICE SERVICE TO ITS USERS.

The Independent Advice Unit (IAU) provides free, confidential, independent, impartial, non-judgemental advice, information and representation to Keele students¹.

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

The full 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 practises and provides information on the legal framework we are working with.

The Independent Advice Unit (IAU) offers a confidential service - nothing you tell us will be shared with any other organisation or individual without your expressed permission. (See 'Breaches of Confidentiality')

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. The Independent Advice Unit 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 IAU Staff, the IAU Manager and the Operations Manager (Services) without that service user's prior expressed consent to disclose such information.

The IAU recognises that all users should be able to access the IAU's services in confidence and that no other person should ever know that they have used the Independent Advice Unit's services.

The Independent Advice Unit recognises 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 IAU can take place outside of the Unit. The Management Committee will not receive details of individual users or their case. The IAU recognises that users need to feel secure in using the IAU's services in

¹ See Code of Practice for current definition of 'student'.

a confidential manner. The IAU 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 should not be discussed in public places even when names are not mentioned.

The Independent Advice Unit will not confirm the user's presence in the centre or use of the centre without obtaining the user's consent.

The Independent Advice Unit is committed to effective statistical recording of service users to enable us to monitor take-up of service and to identify any policy issues arising from advice services. It is the 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 Manager's responsibility to ensure that any Good News Reports are produced in an anonymous form ensuring individuals cannot be recognised.

It is the Manager's responsibility to ensure all ongoing case records are kept in locked filing cabinets. All case records must be locked away at the end of each working day. All information relating to service users will be left in locked cabinets. This includes note books, copies of correspondence, calculation sheets and any other sources of information.

It is the Manager's responsibility to ensure that Independent File Review sheets are held centrally in a locked drawer or filing cabinet.

It is the responsibility of advisors to ensure that where any action is agreed to be taken by the IAU on behalf of a client, that client must firstly sign an authorisation form or email the IAU with authorisation from their Keele account. This should be recorded on the client's file. IAU 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 the IAU when making telephone contact with clients, although if a message is taken and a name is required, we will leave a first name only. IAU 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: the IAU recognises that occasions may arise where individual workers feel they need to breach confidentiality. The IAU recognises, however, that any breach of confidentiality may damage the reputation of the IAU 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 Manager.
2. The worker must discuss with the 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 Manager should take a written note of this discussion.
3. The Manager is responsible for discussing with the worker what options are available in each set of circumstances.
4. The Manager is responsible for making a decision on whether confidentiality should be breached. If the Manager decides that confidentiality is to be breached then they should take the following steps:
5. The Manager should contact the VP Education & Welfare and the Operations Manager (Services) of the Students' Union. The Manager should brief the VP Education & Welfare on the full facts of the case, ensuring they do not breach confidentiality in doing so. The Manager should seek authorisation to breach confidentiality from the Operations Manager (Services).
6. If the Operations Manager (Services) agrees to breaching confidentiality, a full written report on the case should be made and any action agreed undertaken. The Manager is responsible for ensuring all activities are actioned.
7. If the Operations Manager (Services) does not agree to breach confidentiality then this is the final decision of the Independent Advice Unit.
8. In no circumstances should any breach of confidentiality be discussed at this stage with the President. This is to ensure that any future complaints or investigations arising from a breach in confidentiality can be carried out in an independent manner.

The IAU 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.

The policy will be reviewed annually and amendments should be proposed and agreed by the Union Committee.

Date procedure was agreed: ___ January 2011 _____

Date of review: ___ February 2012 _____

Person responsible for review: ___Fay Harris, Advice Unit Manager/Ceri Smith
Operations Manager (Services)_____

THE INDEPENDENT ADVICE UNIT 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 the Unit will remain within the Unit, subject to statutory restrictions.

1.2 Confidentiality rests with the Unit, not individual workers, so it is perfectly acceptable for all workers in the Unit 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 Advice Unit Manager will hold signed copies of the policy.

1.3 The Executive Committee are not covered by the confidentiality policy (except VP Education and Welfare) – and do not have access to case records nor be made aware that an individual has consulted the Unit. Clearly the Executive Committee should be aware of the policy and have an involvement in dealing with any potential breaches of confidentiality – the ultimate responsibility for implementing policies rests with the Executive Committee and workers should be accountable to them.

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 the Unit or is currently in the Unit 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. The Unit 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 the Unit 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 the Unit –always keep a copy of the case record at the Unit 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 6/7 years. When dormant, cases can be boxed alphabetically in year groups and kept in a locked cupboard/room. After 6/7 years since last contact must be shredded/incinerated.

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 the IAU 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 the Unit using electronic mail are to be informed of the following. *“The Independent Advice Unit is happy to advise students and staff using electronic mail. However, the Unit 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 LINDSAY LOAN FUND AND LAZAROUS CHARALAMBOUS INTERNATIONAL FUND

2.8.1 Whilst details surrounding a case, which necessitates a loan from the Lindsay Loan Fund, are treated in accordance with this policy, the fact that the loan has been made cannot. This is due to the internal accounting system within KUSU. Therefore all loan application forms will warn service users:

This loan has been made to you on the understanding that it will be repaid on or before the agreed date. If it remains unpaid after two reminders, details of the amount and who owes it will be passed to our Finance department to instigate recovery action. Due to this and that our accounts are subject to annual audits, the fact that you have a loan from the fund will fall outside our Confidentiality Policy.

2.8.2 Applicants to the Lazarous Charalambous Fund will be similarly informed:

Applications for grants are considered by a panel, the University International Officer and the University Head of Student Finance are members of the panel. In the event of a grant being awarded, your details and the amount awarded will have to be passed to our Finance department to arrange payment, and therefore these details will fall outside of our Confidentiality Policy.

Service users will be informed of the Students' Union charity number 1137380

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. The IAU is committed to effective statistical recording of service users to enable the Unit to monitor the take up of service and identify any policy issues arising about or from advice services. It is the Advice Unit 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 IAU Advisors 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 Advisor to return to the Unit to store records appropriately.

2.10.2 There may be occasions when following an outreach session or an Advisor has been working from home that the Advisor is not able to return to store the files in locked cabinets within the Unit., If this happens the Advisors 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 I.A.U. 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 advisor 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 THE ADVICE UNIT

3.2.1 The police may approach the Advice Unit 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 the Advice Unit – 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 & Advice Unit Managers' 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 The Advice Unit can negotiate with the police or when attending the magistrates court and explain case records are confidential. The Advice Unit 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 THE INDEPENDENT ADVICE UNIT

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 the Independent Advice Unit e.g. theft from the waiting room, following the steps outlined in the section on "Police attending the Advice Unit".

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 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. 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

3.6.1 The Data Protection Act was implemented in October 1998 which brought the UK in line with the European directive on data protection. The legislation applies to manual files as well as 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 practise – 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 advisors 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, IAU advisors 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. Advisors 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 Unit 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 the Unit's services but is unwilling to give notification of their change in circumstance, you should consult the manager 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.

3.8 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 IAU team is subject to threatening, violent or abusive behaviour by the user they will be asked to leave the Unit, or stop contacting the Unit, as appropriate. If a service user is ejected from the Unit and security has to be called this will require a breach of confidentiality. See also IAU Withdrawal of Service Statement.

3.9 CONFLICT OF INTERESTS

3.9.1 A conflict of interest arises where the Unit 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 advisor, 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. Often conflicts are identified through chance conversations.

3.9.4 The most common situations for conflicts to occur are:

- Landlord and tenant
- Issues arising out of a relationship breakdown
- Harassment
- Plagiarism / Collusion
- Neighbour disputes in halls / off campus accommodation
- Union disciplinary procedures

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 IAU’s 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.
- Check third party name – the IAU’s 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

3.9.6 The IAU will offer advice, information and representation to the first person accessing the service, where a conflict or a potential conflict of interest has been identified.

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

3.9.8 The Advisor should explain the Conflict of Interest policy and direct the service user to another agency for help – see the policy on Signposting and Referral.

3.9.9 If the IAU has been advising both parties the IAU Manager should be informed. Ideally, both parties should 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 as per paragraph 3.7.6 and 3.7.7 and that if the case goes further e.g. to a hearing or to court the IAU will cease to act for both parties and that if this is likely the advisor should consider referral at the earliest opportunity.

3.9.11 The nature of conflict of interests is that it can not 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 REHABILITATION OF OFFENDERS ACT

3.10.1 This Act provides ex-offenders with the right not to reveal convictions in most situations when the offence has become “spent” after a rehabilitation period without a further offence.

3.10.2 There are varying rehabilitation periods – the heavier the sentence the longer it takes for a conviction to be spent. For the majority of jobs it makes it unlawful to dismiss an employee or refuse to employ a person because he or she has a spent conviction. It is good practice only to ask potential employees to discuss spent convictions.

3.10.3 There are a number of exemptions to an individual’s rights not to reveal a spent conviction; which broadly relate to work with children, the sick, disabled people and the administration of justice. Given the varied nature of the work the IAU carries out (working with school age children, students with disabilities, working in a one to one setting) we request that future employees must, if asked, disclose convictions including spent ones.

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 Advisor, 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 Advisor 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 Advisors must inform the Advice Unit Manager that information has been passed onto the authorities. The Advice Unit Manager must inform the Operations Manager (Services) when they or any Advisors 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 Advisors 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 IAU Manager and the Operations Manager (Services) 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 Advice Units' Confidentiality Policy:

Name: _____

Signature: _____

Date: _____

Index

- Benefit Agency, 17
- Breaches of Confidentiality, 4
- case records, 9
- child abuse, 2
- CHILD ABUSE, 15**
- Children Act 1989, 15
- Children and Family Social Work teams, 2
- Children and Family Social Work Teams, 16
- conflict of interests, 18, 19, 20
- CONFLICT OF INTERESTS, 18**
- CONTACT WITH A THIRD PARTY/REFERRAL SERVICE, 8**
- CRIMES COMMITTED IN THE INDEPENDENT ADVICE UNIT, 15**
- DATA COLLECTION, 9**
- DATA PROTECTION ACT, 16**
- definition of terrorism, 21
- Deputy General Manager of the Students' Union, 4
- DISCLOSURE OF CRIME, 12**
- Employment Rights Act 1996. *See*
- Executive Committee, 7
- Finance department, 11
- FRAUD ACT. *See* Social Security Administration (Fraud) Act 1997**
- Good News Reports, 3
- Head of Student Finance, 11
- INCOMING/OUTGOING POST, 8**
- Independent File Review, 3, 9
- Landlord and tenant, 18
- Lazarous Charalambous, 11
- LAZAROUS CHARALAMBOUS INTERNATIONAL FUND, 11**
- LEGAL ISSUES, 12
- Lindsay Loan Fund, 11
- LINDSAY LOAN FUND, 11**
- Local Authority, 8
- Management Committee, 3, 6
- Operations Manager (Services), 2, 4, 5, 6, 21
- Outreach and storing records at home, 12**
- PACE, 15
- police, 8, 14, 15, 16, 17
- Police and Criminal Evidence Act 1984 (PACE), 14
- POLICE ATTENDING THE ADVICE UNIT, 14**
- President, 5
- PRIVACY, 9**
- probation officers, 7
- PROVIDING INFORMATION TO THE POLICE, 14**
- REHABILITATION OF OFFENDERS ACT, 20**
- RISK OF HARM, 17**
- Social Policy, 11**
- Social Security Administration (Fraud) Act 1997, 12
- social services, 7
- solicitor, 8
- STORING RECORDS, 9**
- telephone calls, 8, 9
- terrorism, 21
- Terrorism Act 2000, 12
- TERRORISM ACT 2000, 20**
- University, 8
- University International Officer, 11
- USE OF E-MAIL, 10**

VP Education & Welfare, 4

waiting areas, 9