Information Commissioner's Office

Upholding information rights

3rd Floor, 14 Cromac Place, Belfast, BT7 2JB
Tel. 0303 123 1114
www.ico.org.uk

DHSSPSNI
Adult Safeguarding Policy Team
Room A3.5
Castle Buildings
Stormont Estate
Belfast
BT4 3SQ

4 February 2015

Dear Sir/Madam

ICO Response - Consultation on a Draft Adult Safeguarding Policy

We welcome the opportunity to comment on the draft NI Adult Safeguarding Policy ('the policy') for Northern Ireland. As the UK's independent body to oversee and enforce the Data Protection Act 1998 ('the DPA'), the ICO has a vested interest in ensuring any processing of personal data for adult safeguarding purposes is compliant with the DPA. We are therefore pleased to have an opportunity to inform and provide guidance in this respect on the policy from the outset.

We welcome the fact that the draft policy is underpinned by a number of approaches including a rights based approach, a consent-driven approach, and a collaborative approach. In addition, we welcome the overall aim of the policy to provide provision for possible statutory arrangements to improve safeguarding arrangements for adults at risk of harm.

We strongly recommend that a Privacy Impact Assessment (PIA) is carried out on the policy and its related procedures (including any data sharing elements). A PIA is a tool which can help an organisation comply with their data protection obligations as well as meet their clients' expectations of privacy. It will help to assess the benefits that the draft policy might bring to particular individuals or society more widely. The breadth of the policy is wide with far reaching aims of inter-disciplinary and multi-agency collaboration as indicated in Section 1.1.4 and Section 3.2.2. As a large amount of the information being shared is likely to

constitute sensitive personal data as defined within the DPA (e.g. information relating to mental or physical health or to criminal history or allegations of criminal activity), it will be especially important to ensure that the privacy of individuals is protected. For guidance on conducting a PIA please visit Privacy Impact Assessments Code of Practice.

It is recognised that the term 'safeguarding' within the context of the policy encompasses both activity which *prevents* harm from occurring in the first place as well as activity which takes places *when* harm has occurred *or* is likely to occur. In this regard, we have two separate issues we wish to comment on. The first is with respect of *consent*.

It is proposed in the policy that activity/action may take place at times *without* the consent of an individual. We acknowledge that the policy maintains a 'presumption of capacity' in this respect and that consent will normally be sought. However, as indicated in 14.2.8, where there is a need to share information without consent, the adult should be informed accordingly. In addition, individuals should not be asked for consent if it is likely that a decision will be taken to share the information regardless of whether it is given. Any sharing which takes place must also meet the conditions contained under Schedule 2 and Schedule 3 of the DPA or within the Data Protection (Processing of Sensitive Personal Data) Order 2000.

Despite the above, we are mindful of the scope of the proposed sharing and reporting across multi-agencies throughout the public sector and including, community and voluntary groups. We therefore believe it may be beneficial to provide a statutory basis to enable sharing of information for these purposes, to protect adults at risk of harm.

The DPA also requires that processing of information is *fair* for individuals. We would look to the existing adult safeguarding infrastructure and for NIASP to review how arrangements which are compliant with the DPA could be progressed for the purpose of the policy. Part of being fair to an individual includes explaining how the organisation will use their information, so they can be assured their information is being processed in a way that they would reasonably expect. The DPA requires organisations to communicate to individuals the identity of the organisation, the purposes for which the personal data is to be used, and any other information which would be fair in the circumstances.

We have a concern over how the full range of organisations involved in

safeguarding matters will be able to both understand and comply with the fair processing requirements of the DPA. They should ensure that they provide adequate privacy notices to individuals, including the situations where information may be used about them without their consent, as per Section 14.2.8. This is an essential component of DPA compliance.

With regard to the 'collaborative approach' of the policy, we appreciate that in order to effectively safeguard adults and to work in partnership across sectors, sharing information with one another is necessary. The need to have Information Sharing Protocols is referred to in 14.3.2 and these should be derived with due regard to the ICO's statutory Data Sharing Code of Practice addressing issues such as the purposes of the sharing, data quality, security, retention etc. Organisations should also have in place an effective procedure for dealing with breaches of personal data. We appreciate the importance of good record keeping in relation to decisions to share information highlighted within Section 14.2.10. This is especially important if an individual complains about the way their information has/has not been shared as the organisation will have evidence to support their decision making.

One of the strands documented in Section 8.2.3 is the 'effective awareness of adult harm and responsibility to report'. In order for organisations and health professionals to feel confident about sharing information it will be important for them to understand that the DPA provides clear conditions which will allow personal information in certain circumstances to be shared. In addition, reference is made in Section 14.2.7 to circumstances when personal identifiable information "*can be shared*". This should be amended to read "*may be shared*". As indicated in Section 14.2.9, advice should be sought if there are concerns that sharing may increase the risk of harm or when there are other grounds present which may limit sharing.

It is imperative that a 'blanket' approach to sharing information is not adopted, and that any decision to share is taken on a case by case basis. It is important to note that inappropriate disclosures of personal data can lead to severe detriment of an individual. In such circumstances, this may lead to the ICO taking enforcement action against the data controller/s, including the potential of a civil monetary penalty of up to £500,000.

The policy is intended to assist organisations, their staff and volunteers who provide services to adults. Each organisation is likely to be a data controller under the DPA and have responsibility for complying with the DPA and its

requirements. The data controller will be a legal entity who determines the purposes and manner in which the data is to be processed. As such, the data controller must process personal data in line with the 8 'data protection principles' of the DPA.

Organisations should ensure that the personal data they process should be adequate, relevant and not excessive, kept accurate and up to date, and must not be kept for longer than necessary. This is imperative given that information may be shared with other organisations and may be used to make decisions on adult safeguarding cases.

As indicated previously, all organisations involved in safeguarding activity should be aware of their obligations to respond to a subject access request from an individual. The 6th data Principle requires that organisations uphold all other rights under the DPA, including the right to ask for inaccurate data to be corrected. Also, public authorities will also have obligations to provide information under the Freedom of Information Act 2000. Organisations should have a policy in place for responding to requests under the relevant legislation.

The 7th Principle requires that appropriate organisational and technical measures should be taken to keep personal data secure. All organisations involved in data sharing must ensure appropriate security measures for personal data are in place, regardless of whether they are public, private or voluntary sector. This is especially important given that much of the information being shared will likely to be sensitive personal data and therefore will require a higher degree of security. Minimum security standards should be included in the data sharing agreement and must cover the handling and disposal of both manual and electronic records.

Section 9.1.1 of the document indicates the requirement for the HSCB, PHA and HSC Trusts to ensure that all contracts or service level agreements with service providers contain robust governance arrangements. We would emphasise also if a third party provider is processing personal data on behalf of another organisation and acting under their instructions, that there is likely to be implications for the data controller/data processor relationship between the organisations. As such, organisations should be aware that the DPA requires that where the processing of personal data is being carried out by a data processor on behalf of the controller, such processing must be detailed in a written contract and also must detail the security arrangements in place for protecting the personal data (Sch1, Part II (12)). This may be relevant to Section 8.3.5 of the policy.

We are aware that NIASP is the current adult safeguarding structure within Northern Ireland, however there is limited explanation within the policy on the processes that govern this. Further detail on when and how information is shared, the arrangements in place for the secure storage of information, and retention and disposal policies would be useful.

We appreciate there are a number of levels of action proposed within the policy, including risk assessments, referral thresholds and alternative safeguarding responses. This processing of sensitive personal data will need to be robust to ensure compliance with these security conditions. We understand the provisions detailed with respect to regulatory bodies with clear legal provisions, however due regard will need to be given to the scope of the policy. It will be unlikely small financial institutions, small voluntary organisations or leisure clubs providing activities will have either resource or a legal framework to support this. In this regard, there is a high risk of information not being shared fairly or lawfully or being kept secure.

We welcome the fact in Section 8.5 that training of staff and a policy on the management of records, confidentiality and the sharing of information are included in the 'building blocks of good governance'. We would emphasise that there is a need to deliver data protection training to staff to strengthen these existing proposals. We wish to point out that the training of staff is an integral part of effective data protection practices and in particular compliance with the 7th principle in the DPA, the requirement to keep information secure and we would be pleased to work with the Department in promoting this element of work. We further welcome the commitment in Section 15 by NIASP to develop a Regional Adult Safeguarding Training Framework.

Within Section 13 relating to access to justice, we would reiterate the right for individuals to access information which is about them, a right enshrined within the DPA. In addition, it must be the case to ensure fairness that individuals are informed as to what will happen to their information if they give witness statements. We have made similar comments with respect to these provisions during the consultation on the NI Victim Charter in 2014.

We hope these comments have been useful and we look forward to providing further advice and information with respect to the policy in the coming months.

Yours sincerely

Dr Ken Macdonald
Assistant Commissioner for Scotland & Northern Ireland