

Chang Li Chun
request-62422-d91ee928@whatdotheyknow.com

Web www.ukba.homeoffice.gov.uk

21 March 2011

Ref: 17821

Dear Chang Li Chun,

Thank you for your email of 20 February, where you have requested information about Case Worker (UKBA employee) Disciplinary Procedures at UKBA. Your request has been handled as a request for information under the Freedom of Information Act 2000. We are now in a position to provide a full reply to your request.

You asked the following:

Whether you, the UKBA, can publish the details (names) of the caseworkers at Liverpool. Data Protection Act notwithstanding, these are public servants so why can't their names be published? We (the public) pay for them, so we want to know who are these (in effect) our employees.

Whilst it is accepted that the caseworkers are civil servants acting in their official capacity, however the names of these officers is considered personal data. Releasing any information under the FOI Act is deemed as being released in the public domain.

The UK Border Agency has obligations under the Data Protection Act and in law generally to protect personal information.

Section 40(2) of the Freedom of information Act states that information is exempt information if disclosure would breach any of the data protection (DP) principles. The general policy of the Home Office is not to disclose, to a third party, personal information about another person. This is because we have obligations under the Data Protection Act and in law generally to protect this information. Your request for personal information has been considered in line with our obligations under the Freedom of Information (FoI) Act. However, we have concluded that the information you have requested is exempt from disclosure under section 40(2) of the FoI Act. This exempts personal data if disclosure would breach any of the data protection principles.

Your enquiry goes on:

The second question relates to safeguarding an applicant's confidentiality. What Disciplinary procedures are in place at UKBA to safeguard an applicant's confidentiality against any misdemeanour by a caseworker? and in the event a caseworker 'clandestinely steals' the applicants personal information and passes them over to unknown third parties what can and would UKBA do against the caseworker? So state the disciplinary actions actionable against such a caseworker.

I know there are many acts e.g. Official Secrets Act etc these acts mean nothing unless acted upon. So my point is, can you spell out the maximum action/penalty you at UKBA, can and would take against a caseworker (a UKBA employee) who abuses their authority. In other words state your disciplinary procedures against the caseworker.

Some reprimand and them being sacked from their job would not be satisfactory. Would you take them to court, and have the courts impose hefty fines, and basically come down heavily on the miscreant.

The UK Border Agency (UKBA) is committed to making sure all the information it handles is done so in a manner which is consistent with the necessary legislation such as the Data Protection Act, Freedom of Information Act and Public Records Act. In this regard, in June 2008, the UKBA published an Information Charter (available on the UKBA website) which outlined the principles it will follow when it asks members of the public for information (i.e. only asking what is needed, protecting it and making sure nobody has access to it who shouldn't etc) as well as what the UKBA would expect in return from the public (i.e. providing accurate information and advising of any changes of circumstances such as a new address etc).

To support the Charter all UKBA staff are required to undertake mandatory training on effective information management every year. The training emphasises information security is a personal responsibility, that staff should know the rules for handling information and these rules should be followed rigidly (including making certain the necessary authority has been obtained (and legal power secured) before releasing any information to others). As such the UKBA treats any misuse of information or a breach of security procedures very seriously with such misuse warranting potential disciplinary action involving serious or gross misconduct.

Breaching security or IT protocols for any reason, including confidentiality of customer data, is treated very seriously by UKBA and is potentially a gross misconduct offence.

Every misconduct case is dealt with on an individual basis, depending on the facts of what took place, who was involved and any mitigation to be taken into consideration. The misconduct procedure requires a formal investigation and where gross misconduct is suspected, the employee may be suspended from work. If a case is found to answer, the commissioning manager would hold a formal meeting to consider the facts and to decide an appropriate penalty, up to and including dismissal. Every case is different depending upon the facts and cannot be generalised. We do however look at previous similar cases and their outcomes to ensure we are being consistent.

SECURING OUR BORDER CONTROLLING MIGRATION

If there is a criminal element the case will be referred to the security and corruption department and the Police or the Independent Police Complaints Commission (IPCC) may be notified.'

The UK Border Agency expects the highest levels of integrity from its staff. However, on the rare occasion a small number of staff members fall below our expectations and as with many organisations we are at risk the unscrupulous seeking to work for us. We have robust recruitment procedures, strong management practices and appropriate methods of detecting corrupt activity. Any allegations of inappropriate behaviour or corruption are thoroughly investigated and we will take action swiftly where we find members of staff who we believe have broken the law. We always seek to prosecute where it is appropriate to do so and we have a dedicated unit of trained officers who work in close co-operation with the police to investigate internal fraud and corruption."

I hope that this information meets your requirements. I would like to assure you that we have provided you with all relevant information that the Home Office holds.

If you are dissatisfied with this response you may request an independent internal review of our handling of your request by submitting a complaint within two months to the address below, quoting reference 17821. If you ask for an internal review, it would be helpful if you could say why you are dissatisfied with the response.

Information Access Team
Home Office
Ground Floor, Seacole Building
2 Marsham Street
London SW1P 4DF
e-mail: FOIRequests@homeoffice.gsi.gov.uk

As part of any internal review the Department's handling of your information request will be reassessed by staff who were not involved in providing you with this response. If you remain dissatisfied after this internal review, you would have a right of complaint to the Information Commissioner as established by section 50 of the Freedom of Information Act.

Yours sincerely

Freedom of Information Team
UK Border Agency