Deaths during or following police contact annual report

Policies and statements

Last updated: January 2018

Contents

1. Introduction

Becoming the Independent Office for Police Conduct (IOPC)

On 8 January 2018, the IPCC became the IOPC, as set out in the Policing and Crime Act 2017. The Act introduces several changes that we asked for – both to the police complaints system and to the structure and powers of the IPCC.

Since 2013, we have doubled in size and are taking on nearly six times as many independent investigations. Given this level of growth, we asked the Government for a new structure that is better suited to our much expanded organisation. The new structure will have a Director General at its head, supported by two deputies, and a network of regional directors and a director for Wales. As it will no longer be a 'commission', we are taking on a new name.

It's important to note that while our name will change, our role, purpose and independence will not. The IOPC will continue to oversee the complaints system as a whole, to provide an independent appeal mechanism for some complaint investigations carried out by the police, and to carry out our own independent investigations into serious and sensitive cases. We will continue to use what we learn through our work to improve policing.

Reference to the IOPC in this document, also covers the processes and policies that were in practice when we were operating under the name IPCC from 1 April 2004 to 7 January 2018.

The Code of Practice for Official Statistics requires producers of statistical reports to publish a number of statements and policies in relation to their outputs. This document is a collection of those policies which relate to the IOPC annual report 'Deaths during or following police contact: statistics for England and Wales' and those previously published under the IPCC.

We have also published a guidance document for users that details how we collate and categorise deaths for inclusion in the annual report and provides additional information on the content of the report.

The annual death statistics were reviewed by the National Statistician in 2012 who concluded that the figures are produced rigorously and consistently. The annual death report was also assessed by the UK Statistics Authority and in July 2013 the Assessment Committee approved its designation as national statistics for the 2012/13 report and all subsequent releases.

2. Confidentiality and security of data

The following IOPC policies apply to the annual death report and can be found in full at Annex A:

- Information and Communications Technology (ITC) Security Policy
- Information Security Policy,
- Information Risk Management Policy

In addition there are further steps taken to ensure the security of the data used in the annual death report and other data handled by the research team.

- The dataset containing information on the death cases and any associated analysis spreadsheets are limited in access to the research team.
- All data sent to external parties for validation is over a secure network.
- During the writing of the report, checks are in place to ensure that information used to describe the cases is confirmed by the lead investigator. This is also the case when responding to individual questions or queries about the data presented.

3. Statement of administrative sources

The following administrative data sources are used in the production of the death statistics:

- Perito (previously CTMS): This is the IOPC's case management system used by all operational staff to record and progress casework and investigations. CTMS, which had been in place since the creation of the IPCC, was replaced by Perito in March 2013. All relevant data held in CTMS was mapped and migrated to the new system.

- Perito documents (previously TRIM): Previously there was a separate document management system (TRIM) that was used by all operational staff to create and store all case related documents. This has now been migrated to Perito where all case documents are stored.

These systems are covered by the IOPC's polices on information security and risk management attached to this document at Annex A.

The research team, who are responsible for the collation of the death statistics, have been fully engaged in the development of Perito. This has ensured that data required for the report is captured and that existing data is migrated to the new system. The team have also worked with the IOPC's IT provider to design the reports used to extract and analyse data from Perito. Changes to IOPC systems are subject to Management Board approval and overseen by the Information Technology Steering Group (ITSG). The research team were represented at both groups to ensure that the implications for reporting and analysis were considered when system changes were proposed.

The data obtained from these administrative sources is only the first step in the production of the report. All information is checked and verified before inclusion in the final figures. (See Section 6 of this document)

4. Revision policies

This section details the action taken when there are revisions or amends required to the published data in the annual death report.

Routine revisions to published data

Occasionally we are alerted to a death occurring in a financial year after the annual report for that reporting year has been published. This could happen due to a late referral from a police force, or where a death in or following police contact has been redetermined to an independent investigation after publication (see the guidance document for definitions of the death categories). In these instances, the figures in the published annual report will **not** be amended. However, in the subsequent annual report where the trend figures are presented, the previous year's figures will be updated accordingly. This is relevant in two tables - one showing number of fatalities and one showing the number of incidents. Any amends to the figures in these tables will be marked with a footnote explanation.

Managing errors in published data

If an error is noted in the presentation of the figures that is due to human error or occurs during the publication and design process, for example a death is marked against an incorrect force, the published report **will** be amended. The annual death report is not printed, so the PDF version of the report will be updated and a note of explanation of what has changed will accompany the report on the external website. This will occur as soon as practically possible after the error is identified. The report will also be updated on our internal systems and any affected stakeholders will be notified of the change. The relevant table(s) in the associated Excel document will also be revised with an explanatory footnote detailing the change from the previous version.

5. Announcing changes to methods

For any significant changes to the definitions of the data, classifications or methods used, there will be a process of consultation that is proportionate to the size and scope of the annual death report and suggested change. The following section describes the processes for implementing significant changes to the methods or definitions used relating to the data and in the production of the report. The core processes and definitions have not changed in-light of the IPCC being renamed the IOPC.

Any proposed changes to the methods or classifications will be detailed on the IOPC website. Users of the report will be invited to provide feedback about the changes during a consultation period. Feedback will be collected via a form on the IOPC website next to where the annual report is hosted. Key internal and external stakeholders who are known users of the report will be engaged directly with the opportunity to provide comments. The final decision on any changes to the classifications, data or methodology relating to the annual death report rests with the Director of Strategy and Impact at the IOPC.

Once a decision on any changes has been finalised, this will be announced on the IOPC website ahead of the release of the publication. Key internal and external stakeholders will be notified directly via email and provided with detailed information to ensure that they have a full understanding of the change and any impact this may have on the figures. Announcements on consultations and changes will also be made via the IOPC Twitter account if appropriate.

In the trend data presented in the annual report, any changes in the definitions or methods are clearly highlighted and advice is provided on the impact this may have on conducting trend analysis on the data. The guidance document will be updated with detailed descriptions and explanations of any changes that occur.

6. Quality assurance

The statements in this section refer to the six dimensions of the European Statistical System (ESS) Quality Framework and details how the annual death report meets these standards. The key quality measures have been addressed plus any other relevant factors.

Relevance
The annual death report is the only official source of information providing details on deaths in or following police contact for England and Wales.

See the user engagement strategy section of this document for information on how feedback is gathered from users. For details on the key users of the statistics, what feedback we have currently received and how this has influenced the report or data collection see user engagement feedback document.

Refer to the guidance document which details the classifications of the death categories used in the annual report. It also describes the main variables of data reported on, such as cause of death, restraint, mental health and alcohol and drugs.

Accuracy
The key quality accuracy measures set out in the ESS are not applicable to the annual death report. This is because the report does not use a sampling framework; the data is not collected via a survey and therefore sampling error is not applicable; none of the information is based on estimates; and there is no statistical testing.

The first step in identifying death cases is taking a snap-shot of the data stored on the IOPC's case tracking management system, Perito. All associated files on a case are stored on Perito that also forms part of the administrative source data. No information is assumed correct where it has been taken from administrative sources. All information that appears in the annual death report goes through a process of validation with internal operational staff and police forces.

Every effort is taken to find any missing information that is not immediately available from administrative sources as part of the validation process with stakeholders. Users are informed if information on a particular data item is not known in the body of the report and in the tables relating to demographics in the Appendix.

Further information on the process of collecting the data and details of the information published in the annual report, can be found in the guidance document. See the revisions policy above that details how revisions to the data are dealt with in the report.

The annual death report was subject to a formal independent statistical review by the National Statistician in early 2012. The review concluded that the figures are produced rigorously and consistently.

Timeliness and punctuality
The annual report is produced on a financial year basis. The IOPC, when operating as the IPCC, assumed responsibility for collating and publishing annual statistics on deaths from the Home Office in 2004. The first published annual report covered the period 2004/05. The

annual report aims to be published in July, within four months of the end of the period covered in the release. There are no provisional outputs released.

The cases reported on are often subject to ongoing investigations and therefore the administrative data sources are continually being updated. To allow for the writing and publication timetable of the report, the cut-off for taking new information from administrative sources is approximately a month prior to publication.

For customised data requests from existing sources, we aim to respond within a week of receipt of the request. The time taken to respond will depend on the complexity and level of detail required from the requestor. Freedom of Information (FOI) requests are governed by the standard timeframes.

Accessibility and clarity

The guidance document details the data collection and analysis process for producing the annual death report. The datasets are not made publicly available due to the sensitivities of the information. If a user requires additional data or different analysis of the information published in the annual report, they are able to make this request via the channels detailed below and the research team will respond appropriately. All tables and graphs that appear in the annual report are made available on the website in Excel format.

The IOPC's website will state the month of intended publication of the annual death reports at least six-months before publication; the aim is to publish in July. As soon as the release date of publication has been confirmed, around six-weeks prior to release date, the website will be updated with the date. Publication dates will also be announced via GOV.UK which replaced the National Statistics Publication Hub in 2014.

The report is available as a PDF document on the IOPC external website. The IOPC website has an accessibility section that provides information on downloading and viewing PDF files, accessing publications in alternative formats and contact details for discussing further specific accessibility needs. There is also a section on how to adapt the website and change the font size or colour and also provides links to speech enable the website. All tables and charts that appear in the annual death report are available in Excel format on the IOPC external website next to the PDF version of the report.

Users have a number of options to contact the IOPC through general enquiries or directly to the research team via email, all of the relevant contact details are on the IOPC website.

Comparability

The aim of the annual death report is not for it to be compared to other countries or institutions. The figures presented are an accurate reflection of the number and types of deaths that meet the criteria for inclusion within each category that have occurred in the reporting financial year. While comparisons can be made to other countries and institutions, care needs to be taken as the data is unlikely to be directly comparable due to differences in death classification or how other details have been collated. The guidance document provides some links to similar information from other jurisdictions and a list of suggested further reading. Please be cautious that, if produced, figures from other countries may not be directly comparable to the figures produced by the IOPC for England and Wales.

The ethnicity classifications used in the data prior to 2015/16 was based on the ONS 16+1 classification of ethnicity. From 2015/16, ethnicity classifications are based on the ONS 18+1 classification of ethnicity. For reporting, this is then grouped based on the ONS ethnicity 6+1

classification: White, Asian, Black, Mixed, Other and Unknown/Not stated. There is a footnote reference that notes this amend when data is presented by ethnicity in the report and supplementary tables.

Coherence
There are no estimated figures in the annual death report. All the figures are produced in the same method. In 2010/11, the definition of one of the death categories was amended and this is detailed in the guidance document.

7. Pre-release access

Pre-release access to the report and data not in its final form is limited to those essential to the production and publication of the annual death report. The roles that have access to the data or report prior to publication are listed below along with an explanation of their role in the production of the report. This list will be reviewed periodically to ensure that it remains relevant.

- The main producers of the report who are involved in every stage of the process and therefore have access to the raw data, drafts and final copy of the report are:
  - Senior Research Officer; lead on the production of the annual death report.
  - Other members of the research team; support on the production of the annual report.
  - Director of Strategy and Impact; is the Lead Official responsible for statistics at the IOPC. They usually become involved once the first draft of the report is ready but will be aware of early indications from the findings and will be notified of any major concerns with the report. They also set the release date of the report and sign-off the report as ready for publication.
- Individuals who will see the report in draft format:
  - Content and Design team; for proofing prior to publication and will also act as the point of contact for the external designer, if used, who formats the report into IOPC branding. The external designer signs a confidentiality agreement.
  - The IOPC's Director General (this role was performed by the IPCC's CEO and Chair); approval of the report style and presentation and also used to inform the section they write in the IOPC Annual Report which references the death figures, if applicable. They also provide an advisory role to ensure that we have considered any relevant strategic context that we may not be aware of. Neither role has any influence over the production of the figures.
  - The Corporate Media Officer; to write the national press release. Other media team colleagues will also have sight of the report to assist with writing individual press releases for forces and answering queries they receive from forces and journalists. As part of the validation process, the media team will see a list of cases to be included in the report for checking. (The Media Team / Media Officers were previously known as Press Team / Press Officers).
- Individuals who will have sight of initial headline figures and findings:

- Internal management board and commission meetings; a draft of the report *does not* get submitted at this meeting but some headlines are presented, or shared securely by internal email, on a draft set of figures. The figures presented are the initial findings and often will not be the final set of figures following the validation process.

- Individuals who have sight of some of the data:
  - During the verification process of the data with police forces, they each receive a file containing the cases included for their force only for checking and to provide missing information where possible. They do not receive a draft copy of the report.
  - Forces will receive the final list of their cases included in the report 24 hours prior to release. It is helpful that forces are aware of their cases to ensure that they have time to clarify or ask any questions regarding the data presented for their force to accurately respond to questions from the media and members of the public. IOPC Regional Directors and the Director for Wales are also notified of their relevant cases 24 hours prior to release for the same reasons (previously this was provided for IPCC Commissioners).

- The release practices for the annual report, in-line with the code of practice for official statistics, are:

- The month of publication will be stated on the IOPC external website at least six-months prior to publication. As soon as the release date of publication has been confirmed, around six-weeks in advance, the website will be updated with this. GOV.UK will also be updated. The Director of Strategy and Impact at the IOPC determines the day of release of the report with support from the communications team for operational considerations.
- Police forces and other known external stakeholders are notified of the release date by email a week prior to release. Internal IOPC staff are also notified of the release.
- The annual death report will be released on the IOPC website at the standard time of 09.30 on a weekday.
- The GOV.UK statistics page will be updated with a link to the annual report in time for release date.
- On the day of publication, police forces and other key external stakeholders, force press offices and news contacts are emailed a copy of the final report and press release.
- On the day of publication, a copy of the report is made available on the internal website, there is an internal news item alerting of the release an email is sent to key internal stakeholders.

8. User engagement strategy

This section details our user engagement strategy and how we collect and receive feedback on the annual death report. For details on feedback received and how it has influenced the information in the report or the data collection process, please see the user engagement feedback document. This section will be updated with future feedback, our response and impact.

Collecting feedback

- There is a short questionnaire on the annual death report page on the IOPC external website that allows users to provide feedback on their experience of the report. This has been available from the point of release of the 2012/13 annual report. Any feedback received through this method is routinely monitored and published in the user engagement feedback document along with details of any actions taken in response. Our approach in relation to suggested amendments or additions to the report will keep in mind the purpose of the report, restrictions on release of the information due to its sensitive nature and available resource.
- Users also have a number of options to contact the IOPC through general enquiries or directly to the research team via email, all of the relevant contact details are on the website.
- The IOPC, when operating as the IPCC, undertook a review of its approach to the investigation of deaths. This review included a public consultation, independent research with bereaved families, plus a number of interviews and focus groups with key stakeholders. A final report and action plan has now been released and work is ongoing in this area. The feedback is being monitored for any specific comments relating to the production of the statistics presented in the annual death report.
- The findings from the annual death report are presented at meetings with key stakeholders, for example at the Independent Advisory Panel Ministerial Board on deaths in custody, which gives users an opportunity to comment and provide feedback.
- The team periodically reviews requests for information received via Freedom of Information (FOI) requests, Parliamentary Questions, media requests and standard enquiries that relate to information that is contained or related to the report, and uses this to inform reviews of the content or presentation of data.
- Every year the figures from the annual death report were presented at the Capita conference 'Preventing Deaths in Police Care' by the IPCC Commissioner lead on this area (this will likely be conducted by a Regional Director or Director for Wales who leads on deaths in the IOPC). Any questions or comments raised during the conference about the report or the data are filtered back to the Research Team to be considered accordingly.
- The IOPC's internal Customer Relations Management (CRM) system stores contact details of individuals and organisations who have an interest in deaths in custody and other related themes. These are notified of the release of the annual report when it is published, with the opportunity to provide feedback if necessary.
- We will routinely review using online statistical networks and platforms to publish information about the release of the report and engage with a wider range of potential users.

9. Pricing policy

All of the reports produced by the IOPC, and those produced by the IPCC, are free and available to download from the IOPC website in a PDF format. If a hard copy is required a request can be sent to the IOPC (email: enquiries@policeconduct.gov.uk, Switchboard: 0300 020 0096 or see other contact methods) and a copy will be printed (on a standard internal printer) and distributed. This service will not incur a cost.

10. Annex A

A: Information and Communications Technology (ICT) Security Policy

Purpose
The purpose of this policy is

- to ensure the confidentiality of information hosted on our ICT systems;
- to ensure the integrity of information hosted on our ICT systems by assuring its accuracy and completeness;
- to ensure that the information is available when required by users; and
- to ensure that our systems are used in compliance with our policies.

The policy
Our ICT systems must comply with UK legislation, regulatory regimes and Government ICT systems security policies, procedures, standards and guidance.

Our systems must provide cost-effective and proportional protection against breach of confidentiality, while maintaining the integrity and availability of the information we hold.

Any protective measures we apply will be commensurate with the prevailing security risks.

Our systems must be security accredited annually in accordance with Government policy by an external accreditor appointed by us.

Our systems must comply with the Cabinet Office's Security Policy Framework (SPF), and HMG Information Standards 4 and 6. We will take full account of the guidance supplied by the UK National Technical Security Authority (NTSA).

We have a contract with a Managed Service Provider (MSP) who must provide us with ICT systems that are fully compliant with all UK Government security policies.

We will establish with the MSP a joint set of monitoring and reporting processes that ensure that our ICT systems are secure and compliant on a 24 hour a day, 365 days a year basis.

B. Information Security Policy

Purpose
The purpose of this policy is to provide a summary of all our information risk management policies.

It also relates to the Information Risk Management Policy. This shows how information risk assessment is incorporated into our corporate risk model.

Security organisation
We have appointed a Senior Information Risk Owner (SIRO) in accordance with Government policy. This is the Director of Business Services. The SIRO is accountable to the Home Office SIRO for information risk management throughout the organisation.

We have also established an Information and Security Management Group to provide a corporate approach to information security.

We have designated certain senior staff as Information Asset Owners (IAOs). IAOs are responsible to the SIRO for the implementation of information risk management policies and procedures in their areas. As part of the formal assessment of security effectiveness, they are required to investigate and report on security problems, breaches and the security performance of their areas.

All third party suppliers with access to any of our information systems must comply with our information security policies. This includes nominating a Security Point of Contact.

Asset classification and control
All sensitive and personal information assets and other assets associated with the secure management of information must be identified, recorded, valued and assigned to an owner. These assets include:

- information assets – documents, files, evidence, voice recordings, metadata, photographs, video, databases and data files, system documentation, user manuals, training material, operational or support procedures;
- software assets - application software, development tools and utilities;
- physical assets - computer equipment, communications equipment, magnetic media, site security;
- services - computing and communications services.

Each category of assets is to be recorded in an inventory.

Information assets must have a protective marking that reflect their confidentiality, integrity and availability. These protective markings must be assigned in accordance with Government guidance.

Much of our business involves the use of personal information about individuals. We have developed guidance on Privacy Impact Assessments and Information Sharing Agreements.

The Information Commissioner has also issued guidance on good information management and assurance practice.

Personnel Security
Security measures are required to reduce the risks to information systems arising from human error, theft, fraud or misuse of information assets.

Commissioners, staff and staff of third party suppliers will undergo security vetting according to the value of the sensitive information they have access to in the course of their work. Staff of third party suppliers will be required to sign a confidentiality/non-disclosure agreement with the IOPC.

All staff and Commissioners will be given a security briefing as part of the induction process and before being given access to our information systems. They must also attend mandatory annual refresher training.

Third party suppliers with access to our assets will be required to demonstrate that their personnel security measures are consistent with our security policy. They may also have to have an appropriate vetting status and attend our security briefings.

All Commissioners and staff must report all security related incidents to their line managers or through other appropriate channels. All security incidents, software malfunctions and suspected security weaknesses in systems or procedures must be reported.

Our human resource management processes include procedures for dealing with staff who may have breached security policies, procedures, security manuals or other security related guidance documents.

Physical and environmental security
We have physical security measures which address risks to all our assets, including information assets. These measures conform with the requirements of the Government Security Policy Framework.

Preventing unauthorised physical access to our offices is very important particularly where accommodation is shared.

Our physical and environmental measures to protect equipment and information must take account of the risks of accident and everyday hazards of theft, fire, flood and power failures etc.

Remote workers must ensure that the IOPC information assets in their working environment are adequately secured against misuse, loss, theft, and/or damage. They must use properly secured equipment for sensitive work.

Third party suppliers' physical and environmental measures must meet our requirements and standards and they must report any incidents to the Security Manager.

Communications and operations management
We require comprehensive management of our communications and operations systems. Our Managed Service Provider (Steria) is responsible for delivering this.

Operating procedures for our information systems must be documented and maintained. Change control processes are key to the proper management of information systems and these too must be fully documented and complied with.

Responsibilities for the proper operation of our information systems must be documented. Duties must be segregated as much as possible to reduce the risk of negligent or deliberate system misuse.

We require software and procedural controls throughout our information systems to minimise the risk of intrusion of a virus or malicious software.

Connections to our electronic information systems from systems owned by other organisations must be protected in collaboration with the other organisations and compliant, where appropriate, with Codes of Connection and approved by the Security Manager.

C. Information Risk Management Policy

Introduction

The purpose of this document is to give an additional focused policy regarding information risk management. It acts as an annex to the current IOPC Risk Management Policy and provides further specific information particularly for those in Information governance roles.

What are Information Risks

Information is essential to today's society, and to most organisations and departments within government. Information can take many forms – from data sets of confidential personal information through to records of sensitive meetings, personnel records, policy recommendations, correspondence, case files and historical records. Information can be in many formats, from databases through to emails, paper and video. Information is not the same as IT – IT systems are the platforms on which information is often exchanged and managed. Therefore, information risks are not necessarily the same as IT security risks (although managing IT security is usually a critical component of any strategy to manage information risks).

Risk management not only means mitigating risk, but also taking considered risks where the rewards are expected to be greater than any short-term losses. The risks of managing information illustrate this. Information risks have the same characteristics as other risks, and need to be managed with the same degree of strategic consideration.

A risk assessment is essential to prioritise the right actions for each part of government. Some information (e.g. published legislation, official publications, and web publications) rarely carries security risks associated with disclosure – the risks around this information are more likely to be about tampering with the official record, or failure to get sufficient dissemination of key information. This is in contrast with sensitive personal data where risks are more likely to be around disclosure or integrity.

What is Information Risk Management

Information risk management adapts the generic process of risk management and applies it to the **CONFIDENTIALITY, INTEGRITY** and **AVAILABILITY** of information and the information environment.

Information risks are threats to:

- **CONFIDENTIALITY** – Resulting in unauthorised access or disclosure;
- **INTEGRITY** – Resulting in inaccurate, incomplete or corrupted data;
- **AVAILABILITY** – Resulting in authorised users being able to access information when required.

The impact of the realisation of these risks determines the protective marking of the information.

Factoring Information Risk Management into the IOPC

Information risk management should be incorporated into all decisions in day-to-day operations and if effectively used, can be a tool for managing information proactively rather than reactively.

All IOPC staff should be aware and refer to the 10 Golden Rules of Information Security for guidance. Here they will find a quick checklist to provide clarification to how personal data should be handled. If the rules are followed by all users, the risk of information breaches is significantly reduced.

Delivery Partners and Third Parties

The IOPC is aware of its responsibilities to risk manage information assets where these are managed by, or shared with, Delivery Partners and Third Parties and it has modified its commercial contracts in recognition of this. Advice and guidance has also been provided to these partners to ensure adequate security whilst at the same time encouraging appropriate information sharing. Delivery Partners and Third Parties are subject to an annual information risk management audit by the IOPC in order to test compliance and thereby ensure good information management. Where companies fall short they will be given advice and guidance as to how they might improve their management arrangements.

Access control

Our business needs will define staff and Commissioner access to information systems. Information system users will be grouped into user groups for the purpose of managing access to our information systems. The "need-to-know" principle will underpin all access management procedures.

We will create user accounts for users of our information systems. These must be reviewed regularly by administrators to ensure that authorisation processes (including user passwords) remain sound. In particular administrators must check that all user accounts are still required.

Access to all IOPC networked or standalone computer services, and intelligent network devices, must be via a secure log-on process designed to minimise the opportunity for unauthorised access. Each user of a computer system must be uniquely identified to the system. Where passwords are used, they will comply with GSI rules on length and complexity and be managed in a secure manner to ensure their confidentiality and integrity. The process of authentication of a user to a system will include allocation of access rights to the data and facilities needed by the user's business role and vetting status.

TRIM is our electronic document repository. It operates resilient access controls at folder level where users' access to data will be controlled and monitored in order to comply with the Data Protection Act, Freedom of Information Act and other legislation.

Access control measures for users' remote electronic access and contractor remote diagnostics are to be robust in accordance with the security requirements of the Government Secure Intranet (GSI) security policy.

Access control measures for system administrators must be particularly robust to reflect the privileged access they will have to IOPC information systems. Particularly strong physical, environmental and personnel security measures must be used in support of access control measures for system administrators.

Our electronic systems' security measures must include timed lockout processes for inactive terminals.

We will audit users' activities on our information systems in accordance with Government requirements to ensure that it conforms with security policies.

System development and maintenance

Security must be a fundamental element in the development of all our ICT systems. It must also be integral or any proposal from a third party supplier for an information system.

The security of all our systems will be subject to an accreditation process and a third party security health check to ensure that appropriate security measures exist.

Information concerning the development of our information systems will be confined to our staff and third party suppliers. Information concerning the development of system security measures will be even more restricted and only extend to staff and third party suppliers' staff with a "need to know".

We will undertake any required cryptographic and encryption key management in accordance with Government standards and procedures.

Business continuity management
Business Continuity Management will ensure that the work on our highest priority cases and other high priority business activities is able to continue whatever damage impacts on our information assets.

We have a framework of business continuity plans. These plans will be regularly tested and kept under periodic review commensurate with prevailing threats to our assets and changes to our business environment.

Appropriate systems and data backups will be undertaken, securely stored, and periodically tested, to ensure minimum disruption to business processing in the event of an incident requiring systems and or data to be restored to a position prior to the incident. Data back-ups will be taken at least once every 24 hours of normal working operation and stored securely off site.

Compliance
All users are required to comply with all relevant legislation, licensing agreements and policies.

We retain the right to access and review any document or file stored on our equipment and will do so to ensure that no policy, agreement, or legislation is contravened. Such reviews will be undertaken with the authority and knowledge of relevant managers under guidelines produced for monitoring conformance with our access and monitoring policy.

Only authorised users will have access to the e-mail and Internet facilities we provide. Limited personal use is permitted but all use must be in accordance with the Code of Conduct and is not to include distasteful, derogatory or obscene material. Unauthorised access to pornographic or other sites containing offensive material or other serious misuse may result in disciplinary proceedings.