Document Name	Code of Conduct for Governors
Version	1
Document Author (name/title)	Karen Kanee, Head of FT Development
Implementation & Compliance Lead (name/title)	Karen Kanee, Head of FT Development
Responsible committee / director	Council of Governors / Director of Corporate Affairs & Trust Secretary
Approved by	Council of Governors
Date approved	TBC
Date issued	TBC
Review date	TBC
Target audience	Council of Governors
Equality impact assessed (yes/no) (full/screening)	Yes
Protective marking	None

DOCUMENT CONTROL INFORMATION

Version	Date	Author	Status (S/D)	Description of Change
1	TBC	Karen Kanee, Head of FT Development	D	
S = Signed Off D = Draft				
Document Author =				

This document is controlled.

If you would like to suggest amendments to this document please contact the document author.

References:

Yorkshire Ambulance Service:

Business Conduct for Staff – Interests, Gifts, Hospitality and Sponsorship Policy, 2012.

Code of Conduct for the Board of Directors, 2012.

Constitution, (including the Standing Orders for the Council of Governors) 2012.

Standing Orders, Reservation & Delegation of Powers and Standing Financial Instructions, 2012.

Other:

NHS Constitution, 2012. Department of Health.

NHS Foundation Trust Code of Governance, 2010. Monitor: http://www.monitor-nhsft.gov.uk/sites/default/files/Code%20of%20Governance_WEB%20(2).pdf

'The Nolan Report' First Report of the Committee on Standards in Public Life. Committee on Standards in Public Life. 1995. http://www.archive.official-documents.co.uk/document/cm28/2850/285002.pdf.

Your Statutory Duties: A Reference Guide for NHS Foundation Trust Governors, 2009. Monitor: http://www.monitor-nhsft.gov.uk/home/our-publications/browse-category/guidance-foundation-trusts/reports/guidance-governors/your-sta

Contents:

1.0 Introduction & Purpose:

1.1 Governing bodies have a particular duty to observe the highest standards of corporate governance. This includes ensuring and demonstrating integrity and objectivity in the transaction of business, including following a policy of openness and transparency in the dissemination of their decision making. Where issues are not considered in the public domain the reasons for this must be clear and unambiguous.

1.2 To deliver the above, this document outlines the Code of Conduct for the Council of Governors and Individual (herein after referred to as 'the Code') in Yorkshire Ambulance Service.

1.3 Public service values must be at the heart of the National Health Service. High standards of corporate and personal conduct based on a recognition that patients come first. The principles underpinning this Code are drawn from the 'Seven Principles of Public Life', as defined by 'The Nolan Report' and are as follows:

1. **Selflessness :** Holders of public office should act solely in terms of the public interest: they should not do so in order to gain financial or other benefits for themselves, their family or their friends.

2. **Integrity :** Holders of public office should not place themselves under any financial or other obligation to outside individuals or organisations that might seek to influence them in the performance of their official duties.

3. **Objectivity :** In carrying out public business, including making public appointments, awarding contracts, or recommending individuals for rewards and benefits, holders of public office should make choices on merit alone.

4. **Accountability :** Holders of public office are accountable for their decisions and actions to the public and must submit themselves to whatever scrutiny is appropriate to their office.

5. **Openness :** Holders of public office should be as open as possible about all the decisions and actions they take: they should give reasons for their decisions and restrict information only when the wider public interest clearly demands.

6. **Honesty :** Holders of public office have a duty to declare any private interests relating to their public duties and to take steps to resolve any conflicts arising in a way that protects the public interest.

7. **Leadership:** Holders of public office should promote and support these principles by leadership and example.

2.0 Scope & Duties:

2.1 Governors must observe the Code wherever they:

a) conduct the business of the Trust;

b) conduct the business of the Council of Governors;

c) act as a representative of the Council of Governors;

d) act as a representative of the Trust and its Foundation Trust Members.

2.2 The Code shall not have effect in relation to the activities undertaken by members other than in an official capacity, except where their personal conduct could reasonably be regarded as bringing their office as Governor of the Council of Governors or the Trust into disrepute (see point 5 below).

3.0 Code of Conduct for Governors (please also refer to Appendix 1):

3.1 The purpose of this Code is to provide clear guidance on the standards of conduct and behaviour expected of all Governors.

3.2 The Code, with the Code of Conduct for the Board of Directors, the NHS Constitution and Monitors document 'Your Statutory Duties: A Reference Guide for NHS Foundation Trust Governors' forms part of the framework designed to promote the highest possible standards of conduct and behaviours within the Trust. The Code is intended to operate in conjunction with the NHS Foundation Trust Code of Governance, the Trust's Constitution, the Trust's Standing Orders (SOs) and with the Trust's Standing Financial Instructions (SFIs). The Code applies at all times when Governors are carrying out the business of the Trust or representing the Trust.

3.3 The role of the Council of Governors is to hold the Chairman and the Non-Executive Directors individually and collectively to account for the performance of the Board of Directors and represent the interests of the Members of the Foundation Trust as a whole and the interests of the public. The role is set out in detail in the Trust's Constitution & Standing Orders, Standing Financial Instructions, the NHS Foundation Trust Code of Governance and is further addressed in Monitor's Guide for NHS Foundation Trust Governors.

3.4 In carrying out its work, the Council of Governors needs to take account of, and respect, the statutory duties and liabilities of the Board of Directors and individual Directors.

3.5 **Confidentiality** - Governors must comply with the Trust's confidentiality policies and procedures (See Appendix 2).

3.6 **Register of Interests** - Governors are required to register all relevant interests on the Register of Interests (held by the Trust Secretary) in

accordance with the provisions of the Constitution. It is the responsibility of each Governor to update the register if their interests change. A pro-forma is available from the Trust Secretary. Failure to register a relevant interest in a timely manner may constitute a breach of this Code.

3.7 **Conflicts of Interest** - Governors have a duty to avoid a situation in which they have a direct or indirect interest that conflicts or may conflict with the interests of the Trust. Governors have a further duty not to accept a benefit from a third party by reason of being a Governor or for doing (or not doing) anything in that capacity.

3.8 Governors must declare the nature and extent of any interest at the earliest opportunity. If such a declaration proves to be, or becomes, inaccurate or incomplete a further declaration must be made. It is then for the Chairman of the Council of Governors to advise whether it is necessary for the Governor to refrain from participating in discussion of the item or withdraw from the meeting. Failure to comply is likely to constitute a breach of this Code.

3.9 **Interests, Gifts, Hospitality** – Governors must abide by the Business Conduct for Staff – Interests, Gifts, Hospitality and Sponsorship Policy at all times.

3.10 **Meetings** - Governors have a responsibility to attend Council of Governors' meetings. When this is not possible, apologies should be submitted to the Trust Secretary in advance of the meeting. Persistent absence from the Council of Governors' meetings, without good reason, may be grounds for removal from the Council of Governors.

3.11 **Training & Development** - Yorkshire Ambulance Service is committed to providing appropriate training and development opportunities for Governors to enable them to carry out their role effectively. Governors are expected to participate in training and development opportunities that have been identified as appropriate for them.

3.12 To that end, Governors will participate in the appraisal process and any skills audit carried out by the Trust

3.13 **Undertaking & Compliance** - Governors are required to give an undertaking – and to **make a declaration** – that they will comply with the provisions of this Code. Failure to comply with the Code may result in disciplinary action in accordance with agreed procedure.

3.14 **Interpretation & Concerns** - questions and concerns about the application of the Code should be raised with the Trust Secretary or the Chairman. At meetings, the Chairman will be the final arbiter of interpretation of this Code.

3.15 **Review and Revision of the Code** - this Code has been agreed by the Council of Governors. The Trust Secretary will lead periodically, a review of the Code. It is for Governors to agree to any amendments or revisions to the Code.

4.0 Corporate Decision-Making

4.1 The Council of Governors should exercise its responsibilities in a unitary manner. That is to say, decisions should be taken collectively by Governors acting as a body. Governors should not act individually or in informal groupings to take decisions on Council of Governor business on an ad hoc basis outside the constitutional framework of the meetings of the Council of Governors.

5.0 General Obligations: Governors Must:

a) promote equality by not discriminating unlawfully against any person;

b) treat others with respect; and

c) not do anything which compromises or is likely to compromise the impartiality or integrity of those who work for or on behalf of the Trust.

6.0 General Obligations: Governors Must Not:

6.1 a) disclose information given to them in confidence by anyone, or information acquired which they believe is of a confidential nature, without the consent of a person authorised to give it or unless s/he is required by law to do so; nor

b) prevent another person from gaining access to information which that person is entitled to by law.

6.2 Governors must not, in their official capacity or any other circumstance, conduct themselves in a manner which could reasonably be regarded as bringing their office as Governor, the Council of Governors, the Trust, or the NHS into disrepute. Should Governors have concerns about such an issue they must advise the Trust Secretary immediately.

6.3 Governors must not, in their official capacity or any other circumstance, use their position as Governor improperly, to confer on or secure for themselves or any other person an advantage or disadvantage; and must, when using or authorising the use by others of the resources of the Trust:

a) Act in accordance with the Trust's requirements; and

b) have regard to any relevant advice given to them by the Chairman of the Council of Governors, a Director or Directors of the Trust;

c) give the reasons for those decisions.

6.4 Governors must advise the Trust Secretary immediately of any situation they find themselves in which affects their ability to comply with the Trust's Code of Conduct for Governors. In addition, if Governors become aware of any conduct by any other Governors, which they reasonable believe involves a failure to comply with the Code, they must make a written statement to that effect to the Trust Secretary as soon as it is practicable for them to do so.

6.5 Governors with concerns regarding any matter relating to the Council of Governors, the Board of Directors or services within the Trust should raise the

matter formally through the proper internal channels i.e., through the Trust Secretary, Senior Independent Director or to the Chairman of the Council of Governors. In such a situation, a Governor's concern will be addressed promptly and it is expected that Governors do not refer such a matter to the media. Such action, unless it can be soundly justified, is liable to breach the Governor's duty of confidentiality. Disclosures of concern to the media before due procedures are exhausted will rarely, if ever, be justified.

6.6 Should a Governor be approached by the media, to comment on any matters of Trust affairs, activities or developments, it is expected that individual Governors will not feel it appropriate to make a personal statement but will refer the media contact to the Trust Secretary.

6.7 Should the view of the Council of Governors be sought by the media on any matter of the Trust's affairs, activities or developments, such a view should be formulated by the Council of Governors as a whole and issued on their behalf by the Trust Secretary.

6.8 Should an individual Governor feel compelled to express a view to the media on any matter of the Trust's affairs, activities or developments, the individual Governor is expected to preface any comments by a statement that they are expressing a personal view and not the views of the Council of Governors or the Trust.

7.0 DECLARATION (To be completed by all Governors)

In undertaking the role of Governor of Yorkshire Ambulance Service, I declare that:

As a Governor:

1. I will actively support the mission, vision and values of the Trust.
2. I will discharge my roles and responsibilities as a member of the Council of Governors in order for it to fulfil its role as defined in the Trust's Constitution.
3. I recognise that the Council of Governors has no managerial role within the Foundation Trust.
4. I acknowledge that, other than attending meetings, events and in my role as a Governor, I have no greater rights or special privileges that any other member of the Trust.
5. I will observe the Trust's policies on confidentiality.
6. I will act with integrity and objectivity and in the best interests of my constituency and the Trust, without any expectation of personal benefit.
7. I will conduct myself in a manner that reflects positively on the Trust, acting as an ambassador as appropriate.
8. I will accept responsibility for my actions.
9. I will abide by the Trust's policies and procedures and will consult appropriately e.g., with the Chairman or Trust Secretary, if I require clarification on any policy or procedure.

Conflict of Interest

10. I will be honest and act with integrity and probity at all times.
11. I will declare all relevant interest and update my Register of Interest declaration if my circumstances change.
12. I understand that the Register of Governors' interests is a public document that will be available on the Trust's website.
13. **Public & Staff Governors:** If I am a member of any trade's union, political party or other organisation, I recognise that, as a Governor, I will not be representing those organisations (or the view of those organisations) but will be representing the constituency that elected me.
14. **Appointed Governors:** If I am a member of any trade's union, political party or any other organisation other than the one I am representing, I recognise that, as a Governor, I will not be representing those organisations (or the view of those organisations) but will only be representing the organisation that nominated me.

Attendance at Meetings of the Council of Governors

14. I will aim to attend all full meetings of the Council of Governors. When this is not possible, I will submit an apology to the Trust Secretary in advance of the meeting. I will endeavour to attend for the duration of the meeting. I am aware that continued absence at meetings could result in my dismissal as a Governor unless the grounds for absence are deemed to be satisfactory by the Council of Governors.

Dealing with Others

15. I will respect the views of my fellow Governors and value them as colleagues. I will endeavour to be consistent, fair and unbiased.

16. I will treat the Trust's Directors and other employees with respect and in accordance with the Trust's policies.

17. I recognise that the Council of Governors and management have a common purpose i.e., the success of the Trust and will demonstrate my commitment to working as a team member.

18. I will adhere to good practice in respect of conduct in all internal and external meetings and act as an ambassador for the Trust.

19. I will seek to ensure that no one is discriminated against because of their religion, belief, race, colour, gender, marital status, disability, sexual orientation, age, social and economic status or national origin.

Communication

20. I will only speak on behalf of the Trust after seeking advice and express authorisation from the Chairman or Trust Secretary or people acting in these roles. I understand that this commitment relates to both initiating and responding to contact with the media.

Training and Development

21. I will participate in induction events and on-going training and development. I will attend events for which I have signed-up or give sufficient notice of my inability to attend. Such notice must be given to the Trust Secretary in writing (including e-mail).

Visit to Trust Premises

22. If I wish to visit the premises of the Trust in a formal capacity as a Governor, I will liaise with the Trust Secretary to make the necessary arrangements. I understand that notice needs to be given and that any visit needs to fit in with service delivery requirements. I will not make unannounced visits to Trust property in my formal capacity as a Governor. I recognise that informal visits to Trust property are not appropriate.

Compliance

23. I will comply at all times with the Constitution, Standing Orders and Standing Financial Instructions of the Trust.

24. I understand that non-compliance with this Code may result in action being taken against me which potentially includes my dismissal as a Governor. Dismissal will be considered only in the most serious cases of improper personal conduct or where there is improper personal conduct over a sustained period of time.

25. I understand that potential termination of my tenure as a Governor will be considered if I have been given the opportunity but not signed the Code of Conduct for Governors; or that I breach the Code; or otherwise bring the Trust into disrepute either in acting as a Governor or in my wider life.

26. I have read and commit to uphold the seven principles of Public Life as set out by the 'Nolan Committee Report'.

PERSONAL DECLARATION

Declaration:

I, …… (please print full name), have read, understood, and agree to abide by the Code of Conduct for the Council of Governors of Yorkshire Ambulance Service.

Signature: ……

Date: ……

Please sign and return this form to the Trust Secretary (and sign and retain the second copy for your records).

APPENDIX 1

Serious and Less Serious Breaches and Sanctions – as defined by the Council of Governors

1. Definition of a Serious Breach:

a) A breach of the Code that is deliberate.

b) A breach of the Code that is likely to bring the Trust, or the role of Governor, into disrepute.

c) A criminal offence leading to prosecution but excluding minor traffic offences. If a Governor is in doubt about the nature of an offence s/he must refer to the Trust Secretary.

d) Disclosure of information not in the public domain and the release of confidential information or information shared in confidence, to third parties.

2. Sanctions for a Serious Breach:

a) Suspension from office.

b) Removal from office.

3. Imposing Sanctions for a Serious Breach:

a) A Sub-Group of the Council of Governors, comprising the Chairman, Lead Governor, and 3 other Governors – 1 Public, 1 Staff, 1 Appointed, may recommend removal of a Governor(s) to the full Council of Governors (in accordance with the Constitution).

b) Where there has been a serious breach of the Code, the Chairman, in conjunction with the Lead Governor, may take such action as may immediately be required i.e., suspension under the Code, prior to the meeting of the Sub-Group.

4. Definition of a Less Serious Breach:

a) A breach of the Code that is not deliberate, as determined by the Chairman together with the Lead Governor.

a) Misconduct at meetings e.g., disruptive behaviour, rudeness, disrespectful of the views of other Governors, the Chairman and/or Directors. The Chairman will be the arbiter in such circumstances.

b) Non attendance at three consecutive meetings or persistent non-attendance without good reason and/or tendering of apologies. The Chairman will be the arbiter in such circumstances.

5. Sanctions for a Less Serious Breach:

a) Verbal warning.

b) Written warning.

5.1 In either of the above cases, such warning will be recorded by the Trust Secretary on the Governor's Personal File.

5.2 Where there has been cause to issue three warnings to a Governor for less serious breaches of the Code, sanctions for serious breach may be applied.

6. Imposing Sanctions for a Less Serious Breach:

Chairman together with the Lead Governor.

The sanctions and breaches outlined in this Appendix are not exhaustive and should be considered in conjunction with the provisions made within the Constitution.

Yorkshire Ambulance Service NHS
NHS Trust

Data Protection Policy

Version:	3.0 FINAL
Name of originator/author:	David Johnson / Angela Brown
Name of responsible committee/individual:	Information Governance Group
Date issued:	01/04/2010
Review date:	April 2013
Target audience:	All Areas

Version Control:

Version	Dated	Review Date	Status
1.2 FINAL	March 2007	April 2010	Released.
1.3 *draft*	18/02/2010	n/a	Minor amends to update.
1.4 *draft*	08/03/2010	n/a	Further amends to include new process for disclosure.
1.5 *draft*	23/03/2010	n/a	Final formatting, no changes to content.
2.0 FINAL	April 2010	April 2011	Released
3.0	March 2012	March 2013	Inclusion of Security of hard copy data security off site

1 Policy statement

Yorkshire Ambulance Service NHS Trust (the Trust) is committed to a policy of protecting the rights and privacy of individuals (this includes patients, staff and others) in accordance with the Data Protection Act. The Trust needs to process certain information about its staff, patients and other individuals it has dealings with for administrative purposes (e.g. to recruit and pay staff, monitor performance and to comply with legal obligations to funding bodies and government). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The policy applies to everyone working or acting on behalf all staff, temps, contractors and students of the Trust. Any breach of the Data Protection Act 1998 or the Trust Data Protection Policy is considered to be an offence and in that event, YAS disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with the Trust, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that departments/sections who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

2 Background to the Data Protection Act 1998

The Data Protection Act 1998 enhances and broadens the scope of the Data Protection Act 1984. Its purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent.

3 Definitions (Data Protection Act 1998)

3.1 Personal Data

Personal Data is data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Such Data includes name, address, telephone number, id number. It also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

3.2 Sensitive Data

Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing.

3.3 Data Controller

Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

3.4 Data Subject

Any living individual who is the subject of personal data held by an organisation.

3.5 Processing
Any operation related to organisation, retrieval, disclosure and deletion of data and includes: obtaining and recording data, accessing, altering, adding to, merging, deleting data, retrieval, consultation or use of data disclosure, or otherwise making available of data.

3.6 Third party
Any individual/organisation other than the data subject, the data controller (the Trust) or its agents.

3.7 Relevant filing system
Any paper filing system or other manual filing system is structured so that information about an individual is readily accessible. Please note that this is the definition of "Relevant Filing System" in the Act. Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

4 Responsibilities under the Data Protection Act

- The Trust as a body corporate is the data controller under the new Act
- A Data Protection Officer has been appointed who is responsible for day-to-day data protection matters and for developing specific guidance notes on data protection issues for members of the Trust
- The Head of Corporate Affairs is responsible for disclosure of health records and person identifiable information (PII)
- An Information Governance Group (IGG) has been established to advise on data protection issues and provide support for the Data Protection Officer. The IGG is chaired by the Assistant Director for IM&T and reports to the ICT Director and reports to Integrated Governance Committee and the Trust Board
- Directors, The Assistant Directors, Senior Management Group, Heads of Departments/Sections and all those in managerial or supervisory roles are responsible for developing and encouraging good information handling practices within the Trust
- Compliance with data protection legislation is the responsibility of all members of the Trust who process personal information
- Members of the Trust are responsible for ensuring that any personal data supplied to the Trust is accurate and up-to-date.

5 Notification

Notification is the responsibility of the Chief Executive and the Data Protection Officer. Details of the Trust's notification are published on the Information Commissioner's website. Anyone who is, or intends, processing data for purposes not included in the Trust's Notification should seek advice from the Data Protection Officer.

6 Data protection principles

All processing of personal data must be done in accordance with the eight data protection principles:

6.1 Personal data shall be processed fairly and lawfully.

Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

6.2 Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.

Data obtained for specified purposes must not be used for a purpose that differs from those.

6.3 Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.

Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data are given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.

6.4 Personal data shall be accurate and, where necessary, kept up to date.

Data, which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that data held by the Trust are accurate and up-to-date. Completion of an appropriate registration or application form etc will be taken as an indication that the data contained therein is accurate. Individuals should notify the Trust of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Trust to ensure that any notification regarding change of circumstances is noted and acted upon.

6.5 Personal data shall be kept only for as long as necessary.

See Section 12 on Retention and Disposal of Data.

6.6 Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.

See section 7 on data subject rights.

6.7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.

See Section 9 on Security of Data.

6.8 Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Data must not be transferred outside of the European Economic Area (EEA) - the fifteen EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual. Members of the Trust should be particularly aware of this when publishing information on the Internet, which can be accessed from anywhere

in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.

7 Data subject rights

Data subjects have the following rights regarding data processing, and the data that are recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed
- To prevent processing likely to cause damage or distress
- To prevent processing for purposes of direct marketing
- To be informed about mechanics of automated decision taking process that will significantly affect them
- Not to have significant decisions that will affect them taken solely by automated process
- To sue for compensation if they suffer damage by any contravention of the Act
- To take action to rectify, block, erase or destroy inaccurate data
- To request the Commissioner to assess whether any provision of the Act has been contravened.

8 Consent

8.1 Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. The Trust understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

8.2 In most instances consent to process personal and sensitive data is obtained routinely by the Trust (e.g. when a new member of staff signs a contract of employment). Any Trust forms (whether paper-based or web-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain specific consent if an individual's data are to be published on the Internet as such data can be accessed from all over the globe. Therefore, not gaining consent could contravene the eighth data protection principle.

8.3 If an individual does not consent to certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that the processing does not take place.

8.4 If any member of the Trust is in any doubt about these matters, they should consult the Trust Data Protection Officer.

9 Security of data

9.1 All staff are responsible for ensuring that any personal data (on others) which they hold are kept securely and that they are not disclosed to any unauthorised third party (see Section 11 on Disclosure of Data for more detail).

9.2 All personal data should be accessible only to those who need to use it. You should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- In a lockable room with controlled access, or
- In a locked drawer or filing cabinet, or
- If computerised, password protected, or
- Kept on disks which are themselves kept securely.

9.3 Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel.

9.4 Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal.

9.5 This policy also applies to staff who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and students should take particular care when processing personal data at home or in other locations outside the Trust. Therefore the use of paper based information away from YAS premises containing Person Identifiable Information (PII) or any data which is deemed as organisationally sensitive) should be kept to a minimum. This is to reduce the risk of theft or unauthorised exposure. There must be a clear **need** to take

this information off site in the first instance and when doing so it is solely the responsibility of the staff member.

9.6 Staff using PII documents off site must ensure its' security within their home from theft as well as unauthorised access. Where possible it should be stored in a locked container (e.g. a filing cabinet, lockable briefcase). If this is not possible, when not in use it should be neatly filed and stored away. In the event of a data breach, the staff member must inform their line manager and follow the Trusts procedure for reporting such incidents using PRISM

9.7 Staff should assess whether purchasing a lockable cabinet or lockable briefcase is needed. This will be dependent on the frequency of use off site and the level of sensitivity of the information e.g. Safeguarding information would require this level of security.

9.8 The use of scanners may also help in reducing the risk of unauthorised disclosure. It may be appropriate to scan highly sensitive documents onto the Trust computer equipment. This provides the added security built already into the IT systems which prevents access to information in the event of theft.

9.9 All staff must be aware that any related information breach will result in them being required to state why the usage was required in that situation and the efforts they made to protect the information.

9.10 In summary, staff who have a clear business need to use hard copies of documents containing PII off site (e.g at home, conference centres, hotels) must consider the following points:

- Keep usage to a minimum in public areas
- Keep equipment and files locked and out of sight during transit
- Ensure the security of information within the home i.e. it is stored in a locked container (e.g. a filing cabinet, lockable briefcase). If this is not possible, when not in use it should be neatly filed and stored away
- Do not dispose of any documents unless it is shredded
- Make sure that your immediate line manager is aware that you have taken the information off site
- Consider scanning the document then accessing it on YAS IT equipment
- Ensure that the information is returned back on site as soon as possible and filed away accordingly

9.11 If you require any advice on this please speak to your Information Asset Owner (IAO), the Information Governance Manager or Senior Information Risk Owner (SIRO).

10 Rights of access to data

10.1 Members of the Trust and the public have the right to access any personal data which are held by the Trust in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the Trust about that person.

10.2 Any individual who wishes to exercise this right should apply in writing to the Department of Corporate Affairs. The Trust reserves the right to charge a fee for data subject access requests (currently £10 for electronic records and £50 for manual, paper or a mixture of manual and computer records). Any such request will normally be complied with within 40 days of receipt of the written request and, where appropriate, the fee. Please see the ***Procedure for Handling Disclosure Requests under the Data Protection Act (1998) Subject Access, Police, Coroners'*** and others available from the Trust's Data Protection web pages for more detail.

10.3 In order to respond efficiently to subject access requests the Trust needs to have in place appropriate records management practices. For information on records management see the Records Management Policy on the Trust website.

11 Disclosure of data

11.1 The Trust must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter. The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of Trust business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the member of the Trust concerned.

11.2 This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

- The individual has given their consent (e.g. a patient/member of staff has consented to the Trust corresponding with a named third party)
- Where the disclosure is in the legitimate interests of the institution (e.g. disclosure to staff - personal information can be disclosed to other Trust employees if it is clear that those members of staff require the information to enable them to perform their jobs)
- Where the institution is legally obliged to disclose the data (e.g. HR returns, ethnic minority and disability monitoring)
- Where disclosure of data is required for the performance of a contract (e.g. PCTs / Acute Trusts / SHA).

11.3 The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- To safeguard national security*
- Prevention or detection of crime including the apprehension or prosecution of offenders*
- Assessment or collection of tax duty*
- Discharge of regulatory functions (includes health, safety and welfare of persons at work)*
- To prevent serious harm to a third party
- To protect the vital interests of the individual, this refers to life and death situations.

**Requests must be supported by appropriate paperwork.*

11.4 When members of staff receive enquiries as to whether a named individual is a member of the Trust, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member of the Trust may constitute an unauthorised disclosure.

11.5 Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request.

11.6 As an alternative to disclosing personal data, the Trust may offer to do one of the following:

- Pass a message to the data subject asking them to contact the enquirer
- Accept a sealed envelope/incoming email message and attempt to forward it to the data subject.

11.7 Please remember to inform the enquirer that such action will be taken conditionally: i.e. "if the person is a member of the Trust" to avoid confirming their membership of, their presence in or their absence from the institution.

11.8 If in doubt, staff should seek advice from their Head of Department/Section, the Head of Corporate Affairs or the Trust's Data Protection Officer.

12 Retention and disposal of data

The Trust discourages the retention of personal data for longer than they are required. Considerable amounts of data are collected on current staff and patients. However, once a member of staff has left the Trust, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others. The

retention and disposal of records will be in accordance with the Trust's Records Management Policy.

12.2 Staff - In general, electronic staff records containing information about individual members of staff are kept indefinitely and information would typically include name and address, positions held, leaving salary. Other information relating to individual members of staff will be kept by the Personnel Department for 6 years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay etc will be retained for the statutory time period (between 3 and 6 years).

Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for 12 months from the interview date. Personnel may keep a record of names of individuals that have applied for, be short-listed, or interviewed, for posts indefinitely. This is to aid management of the recruitment process.

12.3 Disposal of records - Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion).

13 Publication of Trust information

13.1 All members of the Trust should note that the Trust publishes a number of items that include personal data, and will continue to do so. These personal data are:

- Information published in the Trust calendar including
- Names of all members of Trust committees (including the Board, charities, Committee and Audit Committee)
- Names, job titles and academic and/or professional qualifications of members of staff.
- Awards and honours
- Internal telephone directory
- Staff qualifications, long service awards, etc
- Videos or other multimedia versions of training exercises and ceremonies
- Information in staff magazines (including photographs), annual reports, staff newsletters, etc
- Staff information on the Trust website (including photographs).

13.2 It is recognised that there might be occasions when a member of staff requests that their personal details in some of these categories remain confidential or are restricted to internal access. All individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, the Trust should comply with the request and ensure that appropriate action is taken.

14 Direct marketing

Any department or section that uses personal data for direct marketing purposes must inform data subjects of this at the time of collection of the data. Individuals must be provided with the opportunity to object to the use of their data for direct marketing purposes (e.g. an opt-out box on a form).

15 Use of CCTV

15.1 The Trust's use of CCTV is regulated by a separate policy, the ***Closed Circuit Television Policy and Code of Practice.***

15.2 For reasons of personal security and to protect Trust premises and the property of staff, close circuit television cameras are in operation in certain stations and vehicles. The presence of these cameras may not be obvious. The policy determines how personal data obtained during monitoring will be processed.

16 Academic research

16.1 Personal data collected only for the purposes of academic research must be processed in compliance with the Data Protection Act 1998.

16.2 Researchers should note that personal data processed ONLY for research purposes receive certain exemptions (detailed below) from the Data Protection Act 1998 if:

- The data are not processed to support measures or decisions with respect to particular individuals *AND*
- If any data subjects are not caused substantial harm or distress by the processing of the data.

16.3 If the above conditions are met, the following exemptions may be applied to data processed for research purposes only:

- Personal data can be processed for purposes other than that for which they were originally obtained (exemption from Principle 2)
- Personal data can be held indefinitely (exemption from Principle 5)
- Personal data are exempt from data subject access rights where the data are processed for research purposes and the results are anonymised (exemption from part of Principle 6 relating to access to personal data).

16.4 Other than these three exceptions, the Data Protection Act applies in full. The obligations to obtain consent before using data, to collect only necessary and accurate data, and to hold data securely and confidentially must all still be complied with.

16.5 Notes to researchers - Whilst the Act states that research may legitimately involve processing of personal data beyond the originally stated purposes, the Trust hopes that, wherever possible, researchers will contact participants if it is intended to use data for purposes other than that for which they were originally collected.

16.6 Although the Act allows personal data processed only for research purposes to be kept indefinitely, researchers are asked to refer to the Trust's Policy on Records Management.

16.7 For those departments which gather sensitive personal data (as defined by the Act, see Section 3 on Definitions), extra care should be taken to ensure that explicit consent is gained and that data are held securely and confidentially so as to avoid unlawful disclosure.

16.8 Publication - Researchers should ensure that the results of the research are anonymised when published and that no information is published that would allow individuals to be identified. Results of the research can be published on the web or otherwise sent outside the European Economic Area but if this includes any personal data, the specific consent of the data subject must, wherever possible, be obtained.

17 Monitoring and Compliance

The Information Governance Group will seek assurance that data protection systems and processes are managed in accordance with this Policy by the following means:

- the Trust's progress against its strategic and corporate objectives
- the IGG work programme
- compliance with current legislation and guidance
- the annual review of this Policy
- weekly reporting to the Director of Standards and Compliance and to the Weekly Incident Review Group (WIRG) on subject access requests for medical records by third parties investigating a claim against the Trust.
- fortnightly reporting to the Executive Team
- monitoring activity in the Integrated Performance Reports to Trust Board
- Corporate Affairs will monitor activity and make half yearly reports to IGG by completing audits of the points identified above.

18 Related documents

Procedure for handling Disclosure Subject Access Requests under the Data Protection Act:
Subject Access, Police, Coroners' and Others
Subject Access Request Procedure
Subject Access Request Form
Records Management Policy
Publication Scheme

19 Further information

Information Commissioner's Webpage
On-Line Data Protection Seminars (Information Commissioner's Office)