NHS
Health Education England

Data Protection policy

Version:	1.0
Ratified by:	HEE Executive Team
Date ratified:	29 May 2018
Name and Title of originator/author(s):	Chris Brady, Head of Public and Parliamentary Accountability
Name of responsible Director:	Lee Whitehead
Date issued:	29 May 2018
Review date:	June 2019
Target audience:	All HEE staff
Document History:	Version 1.0

Developing people
for health and
healthcare

www.hee.nhs.uk

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet, and copied to the internet, is the controlled copy. Any printed copies of this document are not controlled.

As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

Executive Summary

This policy is required to ensure all HEE staff are aware of their responsibilities under the General Data Protection Regulation, which came into effect on 25 May 2018. The policy outlines how HEE complies with the core principles of the GDPR.

Contents

1. Introduction

1,1 Health Education England (HEE) is required to keep and process certain information about its trainees and staff in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

1.2 HEE may, from time to time, be required to share personal information about its staff or trainees within services across HEE and with other third party organisations such as the Department of Health, Higher Education Institutions, clinical placement providers, colleges, faculties, other HEE local offices, the GMC, NHS trusts/Health Boards/Health and Social Care Trusts, approved academic researchers and other NHS and government agencies where necessary, to provide the best possible training and education and to ensure that we discharge HEE's responsibilities for employment and workforce planning for the NHS. This will be on a legitimate need to know basis only. We may also share information, where necessary, to prevent, detect or assist in the investigation of fraud or criminal activity, to assist in the administration of justice, for the purposes of seeking legal advice or exercising or defending legal rights or as otherwise required by the law.

2. Purpose

2.1 This policy is in place to ensure all staff are aware of their responsibilities and outlines how HEE complies with the core principles of the GDPR, which are outlined in section 6 below.

2.2 Organisational methods for keeping data secure are imperative, and HEE believes that it is good practice to keep clear practical policies, backed up by written procedures. This policy complies with the requirements set out in the GDPR, which came into effect on 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

3. Scope

3.1 This policy is relevant to all HEE staff. It covers all activities carried out by HEE that involve the use of personal data.

4. Definitions

DPO: Data Protection Officer
DPIA: Data Protection Impact Assessment
FOI: Freedom of Information
GDPR: General Data Protection Regulation
PIA: Privacy Impact Assessment
SAR: Subject Access Request

5. Duties

5.1 The Chief Executive Officer has overall responsibility for the Data Protection Policy within HEE. The implementation of, and compliance with, this policy is delegated to the Data Controller (Director of People and Communications) and the Data Protection Officers. The Data Protection Officers will report data protection issues to the Data Controller who will have responsibility for bringing these to the attention of HEE's Executive Team.

5.2 The Data Protection Officer role includes:

- Maintaining registrations
- Facilitating training sessions
- Dealing with subject access requests
- Acting as initial point of contact for any data protection issues which may arise within HEE
- Providing reports to the HEE Executive Team as required
- Auditing GDPR compliance
- Facilitating action in areas identified as being non-compliant
- Assisting with complaints concerning data protection breaches
- Acting as the interface between GDPR and Freedom of Information

5.3 The day to day responsibilities for enforcing this policy will be devolved to application/system managers and other nominated personnel. In order to fulfil their roles, the Data Protection Officers in conjunction with the Data Controller will ensure that regular training is provided to remind these personnel of these responsibilities and the most effective way of ensuring adequate information security and confidentiality.

6. Main Body of Policy

6.1 Legal framework

6.1.1 This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

6.1.2 This policy will also have regard to the following guidance

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

6.2 Applicable data

6.2.1 For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, or an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

6.2.2 Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

6.3. Principles

6.3.1 In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6.3.2 The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

6.4. Accountability

6.4.1

- HEE will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.
- HEE will provide comprehensive, clear and transparent privacy notices.
- Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.
- Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

6.4.2 HEE will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

6.4.3 Privacy Impact Assessments/Data protection impact assessments will be used, where appropriate.

6.5 Data protection officer (DPO)

6.5.1 Two DPOs have been appointed in order to:

- Inform and advise HEE, its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor HEE's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.
- The DPOs will report to the highest level of management at HEE which is the Chief Executive.
- The DPOs will operate independently and will not be dismissed or penalised for performing their task.
- Sufficient resources will be provided to the DPOs to enable them to meet their GDPR obligations.

6.6 Lawful processing

6.6.1 The GDPR requires that data controllers and organisations that process personal data demonstrate compliance with its provisions. This involves publishing our basis for lawful processing.

6.6.2 As personal data is processed for the purposes of HEE's statutory functions, HEE's legal bases for the processing of personal data as listed in Article 6 of the GDPR are as follows:

- 6(1)(a) – Consent of the data subject

6(1)(b) – Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

6(1)(c) – Processing is necessary for compliance with a legal obligation

6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

6.6.3 Where HEE processes special categories of personal data, its additional legal bases for processing such data as listed in Article 9 of the GDPR are as follows:

9(2)(a) – Explicit consent of the data subject

9(2)(b) – Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law

9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

9(2)(g) – Processing is necessary for reasons of substantial public interest

9(2)(h) – Processing is necessary for the purposes of occupational medicine, for the assessment of the working capacity of the employee, or the management of health and social care systems and services

9(2)(j) – Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

6.6.4 Special categories of personal data include data relating to racial or ethnic origin, political opinions, religious beliefs, sexual orientation and data concerning health.

6.6.5 Please note that not all of the above legal bases will apply for each type of processing activity that HEE may undertake. However, when processing any personal data for any particular purpose, one or more of the above legal bases will apply.

6.6.6 Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
    - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
    - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
    - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
    - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional. Reasons of public interest in the area of public health, such as protecting against serious cross-border

threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.

- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

6.7. Consent

6.7.1 Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

6.7.2 Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

6.7.3 Where consent is given, a record will be kept documenting how and when consent was given.

6.7.4 HEE ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

6.7.5 Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

6.7.6 Consent can be withdrawn by the individual at any time.

6.8. The right to be informed

6.8.1 HEE's privacy notice is available via its website to individuals in regard to the processing of their personal data. It is written in clear, plain language which is concise, transparent, easily accessible and free of charge.

6.8.2 In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, and where applicable, the controller's representative and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
- Withdraw consent at any time.
- Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

6.9 The right of access

6.9.1 Individuals have the right to obtain confirmation that their data is being processed. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

6.9.2 HEE will verify the identity of the person making the request before any information is supplied.

6.9.3 A copy of the information will be supplied to the individual free of charge; however, HEE may impose a 'reasonable fee' to comply with requests for further copies of the same information.

6.9.4 Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

6.9.5 Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

6.9.6 All fees will be based on the administrative cost of providing the information.

6.9.7 All requests will be responded to without delay and at the latest, within one month of receipt.

6.9.8 In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

6.9.9 Where a request is manifestly unfounded or excessive, HEE holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

6.9.10 In the event that a large quantity of information is being processed about an individual HEE will ask the individual to specify the information the request is in relation to.

6.10 The right to rectification

6.10.1 Individuals are entitled to have any inaccurate or incomplete personal data rectified. Where the personal data in question has been disclosed to third parties, HEE will inform them of the rectification where possible.

6.10.2 Where appropriate, HEE will inform the individual about the third parties that the data has been disclosed to.

6.10.3 Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

6.10.4 Where no action is being taken in response to a request for rectification, HEE will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

6.11 The right to erasure

6.11.1 Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

6.11.2 Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

6.11.3 HEE has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

6.11.4 Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

6.11.5 Where personal data has been made public within an online environment, HEE will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

6.12 The right to restrict processing

6.12.1 Individuals have the right to block or suppress HEE's processing of personal data. In the event that processing is restricted, HEE will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

6.12.2 HEE will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until HEE has verified the accuracy of the data
- Where an individual has objected to the processing and HEE is considering whether its legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead

- Where HEE no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

6.12.3 If the personal data in question has been disclosed to third parties, HEE will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

6.12.4 HEE will inform individuals when a restriction on processing has been lifted.

6.13 The right to data portability

6.13.1 Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

6.13.2 Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

6.13.3 The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or when processing is carried out by automated means

6.13.4 Personal data will be provided in a structured, commonly used and machine-readable form.

6.13.5 HEE will provide the information free of charge.

6.13.6 Where feasible, data will be transmitted directly to another organisation at the request of the individual.

6.13.7 HEE is not required to adopt or maintain processing systems which are technically compatible with other organisations.

6.13.8 In the event that the personal data concerns more than one individual, HEE will consider whether providing the information would prejudice the rights of any other individual.

6.13.9 HEE will respond to any requests for portability within one month.

6.13.10 Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

6.13.11 Where no action is being taken in response to a request, HEE will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

6.14 The right to object

6.14.1 HEE will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

6.14.2 Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

6.14.3 Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- HEE will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where HEE can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

6.14.4 Where personal data is processed for direct marketing purposes:

- HEE will stop processing personal data for direct marketing purposes as soon as an objection is received.
- HEE cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

6.14.5 Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, HEE is not required to comply with an objection to the processing of the data.

6.14.6 Where the processing activity is outlined above, but is carried out online, HEE will offer a method for individuals to object online.

6.15 Privacy by design and privacy impact assessments

6.15.1 HEE will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how HEE has considered and integrated data protection into processing activities.

6.15.2 Data protection impact assessments (DPIAs) or privacy Impact Assessments (PIAs) will be used to identify the most effective method of complying with HEE's data protection obligations and meeting individuals' expectations of privacy.

6.15.3 PIAs/DPIAs will allow HEE to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to HEE's reputation which might otherwise occur.

6.15.4 A PIA/DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

6.15.5 A PIA/DPIA will be used for more than one project, where necessary.

6.15.6 High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

6.15.7 HEE will ensure that all PIAs/DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

6.15.8 Where a PIA/DPIA indicates high risk data processing, HEE will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

6.16 Data breaches

6.16.1 The term ‘personal data breach’ refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

6.16.2 The DPOs will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their mandatory.

6.16.3 Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

6.16.4 All notifiable breaches (including Serious Incidents Requiring Investigation) will be reported to the relevant supervisory authority within 72 hours of HEE becoming aware of it.

6.16.5 The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

6.16.6 In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, HEE will notify those concerned directly.

6.16.7 A ‘high risk’ breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

6.16.8 In the event that a breach is sufficiently serious, the public will be notified without undue delay.

6.16.9 Effective and robust breach detection, investigation and internal reporting procedures are in place at HEE, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

6.16.10 Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach

- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

6.16.11 Failure to report a breach when required to do so will result in a fine, as well as a fine for the breach itself.

6.17 Data security

6.17.1 Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

6.17.2 Confidential paper records will not be left unattended or in clear view anywhere with general access.

6.17.3 Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

6.17.4 Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

6.17.5 Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

6.17.6 All electronic devices are password-protected to protect the information on the device in case of theft.

6.17.7 Where possible, HEE enables electronic devices to allow the remote blocking or deletion of data in case of theft.

6.17.8 Staff will not use their personal laptops or computers for HEE purposes.

6.17.9 All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

6.17.10 Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

6.17.11 Relevant/sensitive circular emails are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

6.17.12 When sending confidential information by fax, staff will always check that the recipient is correct before sending.

6.17.13 Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from HEE premises accepts full responsibility for the security of the data.

6.17.14 Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

6.17.15 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of HEE containing sensitive information are supervised at all times.

6.17.16 The physical security of HEE's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

6.17.17 HEE takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

6.17.18 The Data Protection Officer is responsible for continuity and recovery measures are in place to ensure the security of protected data.

6.18 Publication of information

6.18.1 HEE publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Annual reports
- Financial information

6.18.2 Classes of information specified in the publication scheme are made available quickly and easily on request.

6.18.3 HEE will not publish any personal information, including photos, on its website without the permission of the affected individual.

6.18.4 When uploading information to HEE's website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

6.19 Photography

6.19.1 HEE understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

16.19.2 HEE will always indicate its intentions for taking photographs and will retrieve permission before publishing them.

16.19.3 If HEE wishes to use images/footage of individuals in a publication, such as HEE's website, or other publications written permission will be sought for the particular usage.

6.20 Data retention

6.20.1 Data will not be kept for longer than is necessary.

6.20.2 Unrequired data will be deleted as soon as practicable.

6.20.3 Some educational records relating to former trainees or staff members may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

6.20.4 Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

7. Equality Analysis

7.1 As a public body, subject to the Equality Act 2010, HEE will give due regard to the aims of the Public Sector Equality Duty when making data governance policy decisions.

8. Education and Training Requirements

8.1 All staff will undertake mandatory data security training on an annual basis.

8.2 Ongoing data security training and updated training and guidance material will be provided by HEE's Data Protection Officers.

9. Monitoring Compliance and Effectiveness

9.1 HEE's Data Protection Officers will undertake data protection audits in order to monitor compliance with the policy.

9.2 Compliance with this policy will also be monitored by the Information Governance steering Group together with internal audit reviews where necessary.

9.3 The Data Protection Officers are responsible for the monitoring, revision and updating of this policy document on an annual basis, or sooner should the need arise.

10. Associated Documentation

10.1 This policy will be implemented in conjunction with the following other HEE policies:

- E-safety Policy
- Freedom of Information Policy
- Records management policy
- Information governance policy
- Information risk management policy