Mary Ward Settlement

Data and Records Management Policy

Document status

Status	Approved by the Audit and Risk Committee
Version	1.5
Date	May 2018
Author	Allister Duncan, Head of Finance and Resources
Review	Every 3 years
Distribution	All staff

1. Purpose

1.1 The purpose of the policy is to set out how the Settlement manages the collection, retention, use of and disposal of data, documents and other information.

1.2 Complying with this policy is important not only in order for the Settlement to meet its legal obligations, but also to ensure that everyone we hold data on; whether students, clients, staff, trustees or anyone else; is treated fairly through the holding of that data, the way it is used and the manner in which it is disposed of.

1.3 Efficient and effective management of data and records is also a key element in the efficient and effective management of the Settlement and the range of services that are provided. All staff have a responsibility in this area, particularly when making a decision to collect information, or to collect it in a new format, for the first time.

1.4 The Settlement's Data Protection Officer (DPO) is the Assistant Chief Executive. Anyone who requires advice and guidance on any issue relating to this policy, and its implementation, should consult with the DPO in the first instance.

2. Scope

2.1 This policy applies to all areas of the Settlement and covers documents and data that are held in both electronic and paper format.

2.2 The policy incorporates the Settlement's responsibilities under legislation, primarily the General Data Protection Regulations (2016) [GDPR] and the Freedom of Information Act (2000) [FoI].

2.3 The General Data Protection Regulation is due to be implemented in the UK in May 2018. Although many of the principles underpinning the 1998 Act will remain in the new regulation there will additional responsibilities for data holders/processors and rights for data subjects. This does mean that this policy will need to be reviewed in late 2018/early 2019 once the impact of GDPR can be assessed.

3. Definitions

3.1 The key terms used in this policy are defined in the Glossary of Terms (Appendix A). These definitions are designed to be consistent with their use in the GDPR.

3.2 Personal data held by the Settlement principally concerns the following groups:

i) staff;
ii) volunteers;
iii) trustees;
iv) students;
v) other service users; and
vi) suppliers.

4. Principles

4.1 Personal data processed by the Settlement will abide by the general principles set out in the GDPR. These principles are set out in Appendix B.

4.2 No personal data will be made available to any third party unless (a) there is a legal obligation to disclose it, most often this being a contractual requirement imposed by the funder; or (b) the relevant data subject has given approval to disclosure or (c) disclosure is considered to be in the Settlement's legitimate interest, which is not outweighed by any potential prejudice to the affected data subject's interests. This means, among other things, that we will not sell, or pass on, personal data purely for financial gain. However we do use the personal data we hold to contact data subjects with newsletters and these do include requests to support the Settlement in a number of ways, including financially. Where there is an on-going relationship with the data subject, for example with students, and they have been judged as to expect such communications, then the Settlement will use the legitimate interest basis for this type of contact.

4.3 Any deliberate misuse of personal data may be considered to be a disciplinary offence and may be considered to be gross misconduct, depending upon the circumstances.

4.4 Under GDPR, the Settlement, as the Data Controller, is accountable for the personal data we process. This means that for each type of personal data held we will be able to demonstrate that we comply with the requirements of the GDPR.

5. Responsibilities

5.1 Trustees

The trustees are responsible for ensuring that the Settlement has a comprehensive policy on data and records management that, if properly implemented, will enable the Settlement to meet all of its responsibilities in this area and will help support the achievement of its mission.

5.2 All Staff are responsible for:

i) Ensuring that personal data about them, held by the Settlement, is accurate and up to date;

ii) Informing the data owner of any errors or inaccuracies that they may become aware of through their use of personal data;

iii) Informing the Data Protection Officer of any failure to comply with this policy that they become aware of; and

iv) Reporting to the Data Protection Officer any breach of security.

5.3 Staff who are data owners are responsible for:

i) Recording information correctly; correcting any known errors or inaccuracies; ensuring that data is only used for previously agreed purposes; providing any relevant data in response to legitimate access to information requests; taking reasonable steps to ensure that the agreed level of security for the data is maintained; and that data is deleted in line with the policy; and

ii) When establishing any new collection of data (or designing any new format of data collection) that the requirements of this policy are fully met.

5.3 The Senior Management Team is responsible for ensuring:

i) That the agreed policy is implemented across the Settlement; and

ii) That appropriate training is made available to all staff, include general awareness raising for all staff and specific training for data owners. Training will be mandatory for all permanent members of staff.

5.4 The Data Protection Officer, will be responsible for:

i) Ensuring that the policy is updated in line with any changes of legislation or operational requirements;

ii) That the policy is reviewed every 3 years; and

iii) Where any major changes are proposed to way data is collected, held, analysed or disposed of, that an impact assessment is carried out; and

iv) That any breaches are reported to the Information Commissioners Office within the prescribed 72 hours.

6. Security

6.1 The security of electronic data is covered by the IT Security and Electronic Communications Policy.

6.2 Paper records will be given the same level of security consideration as electronic records. Financial information, particularly where unauthorised access could give rise to a potential financial loss to the data subject, and sensitive personal data will only be kept in a locked environment.

6.3 All personal data and data key to the Settlement's operations held in electronic form will be backed up on a regular basis. Any paper records adjudged to be critical will have electronic copies made.

7. Meeting our obligations under the General Data Protection Regulations (2016)

7.1 Duties under the Act

7.1.1 The General Data Protection Regulations (GDPR) governs the collection, storage, processing, disclosure and disposal of personal data. Some types of personal data are categorised as special (see Appendix C) and have a tighter set of criteria applied in terms of how they should be processed.

7.1.2 In order to comply with the regulations, the Settlement is required to identify the types of personal data that it holds and to show that, for each type, it has met its obligation namely:

i) That it has determined the legal basis for processing the data (see Appendix D);

ii) That the DP principles (Appendix B) have been met;

iii) That the data subjects concerned have been properly informed (Appendix E);

iv) That the data is kept in an appropriately secure environment; and

v) That the data is being effectively managed so that it remains accurate and up to date and that it is disposed of when it is no longer required.

7.1.3 In addition to the management of the personal data it processes, the following sections address how the Settlement meets these further requirements:

i) The rights of data subjects;

ii) Subject Access Requests;

iii) Dealing with data breaches;

iv) DP by design and DP Impact Assessments

7.2 Consequences of a failure to comply

7.2.1 Data security is increasingly recognised as a major issue, and numerous high profile cases, including the misuse of data by some charities in their fundraising activities, have put this subject very firmly in the public spotlight. The intensity of interest in this is only likely to grow and, consequently, so will the negative impact on an organisation's reputation of any failure to manage its data effectively.

7.1.4 The Information Commissioners Office (ICO), the body responsible for overseeing compliance with GDPR, has powers to levy fines on organisations for failures. Under GDPR the potential size of these fines has grown enormously. There are two tiers of fines: for less serious offences, the maximum is the greater of 2% of total turnover or 10 million euros; for more serious failures, the maximum is double this.

7.3 Rights of data subjects

7.3.1 The Settlement, through the Data and Records Management Policy and appropriate training, is committed to ensuring that all staff understand their responsibilities as far as the rights of data subjects are concerned.

7.3.2 Under the GDPR there are a number of specific rights, outlined below, that may be relevant in dealing with data subjects:

i) *The right to be informed*

There is an expanded list of information that must be provided (see Appendix E). For each set of personal data that is held there must be an agreed method of communicating all of the required information.

ii) *The right of access*

Requests to access personal data should be responded to as soon as possible and within one month at the latest. (See following section 7.4)

iii) *The right to rectification*

As far as possible there should be a process in place that automatically updates any personal data that may have changed. Any data subject will have the right to request a change in any of their personal data if it is not correct.

iv) *The right to erasure*

This right is dependent on the legal basis for processing the data. Any request for the erasure of data will need to be carefully weighed against the legitimate needs of the organisation. Decisions will be made by the DPO. Any appeal against the DPO's decision will be considered by the Warden.

v) *The right to restrict processing*

This right exists in specific circumstances. Again, the right of the data subject will need to be weighed against the legitimate needs of the organisation. The decision making and appeal process will be the same as the right to erasure.

vi) *The right to object*

Data subjects have the right to object to processing which is carried out for the legitimate purposes of the Settlement or for direct marketing. In the case of the first the Settlement can refuse if the needs of the organisation outweigh those of the individual. In the case of the second the Settlement cannot refuse the request.

7.4 Subject access requests

7.4.1 Access requests can be made by anyone for whom the Mary Ward Settlement holds personal data.

7.4.2 Requests should be forwarded to the DPO in writing (email is acceptable). The DPO will take reasonable steps to verify that the request has actually come from the data subject concerned.

7.4.3 The DPO will seek to engage with the data subject as to the scope of the request if there is any doubt as to the actual data being requested. The Settlement is committed to providing, wherever possible, the information that is actually required rather than simply relying on the wording of the request.

7.4.4 Requests will be replied to within the statutory period of one month. Where possible the response time will be less than this. In exceptional cases the time limit can be extended by up to two months if it is a multiple and/or very complex request.

7.4.5 Under GDPR the data subject is entitled to be given:

i) A copy of all of the records held;
ii) A description of the data held;
iii) The reason(s) for the data being processed;
iv) The origin of the data (if not provided by them);
v) Who has been given the data or who may be given it; and
vi) How long the data is expected to be kept.

7.4.6 Any data subject who is not content with the accuracy or completeness of the response to their request for information has the right to appeal to the Warden, within 10 working days of receipt of the response to their original request.

7.4.7 If the data subject is not satisfied with the response from the Warden then they will be advised of their right to complain to the Information Commissioner's Office.

7.4.8 External examination scripts are exempt from access requests. However, wherever possible, students requesting access to their scripts will be shown them.

7.5 Dealing with data breaches

7.5.1 What is a data breach?

A data breach is defined as a security incident that has affected the confidentiality, integrity or availability of personal data. There will be a breach whenever personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and that unavailability has a significant negative effect on the individual.

Seeing the data is sufficient to warrant the unauthorised access being defined as a breach. However, it is also likely to include the ability for someone to corrupt the data, i.e. to amend or delete it and/or to copy it. In order to be a reportable breach, the unauthorised access only has to take place and there is no requirement for it to actually be used for any damaging purpose.

7.5.2 *What data breaches should be reported?*

Any data held by the Settlement that is breached should be reported to the DPO, or other member of SMT, as soon as it is reasonably possible to do so. Preferably this should be done by email or alternatively by telephone.

All staff have a responsibility to report data breaches as soon as they become aware of them.

The DPO, or other member of SMT, will report the breach to the ICO within 72 hours of being notified of it if the breach is judged to represent any risk to the rights and freedoms of the data subjects. Any breach involving encrypted data does not need to be reported to the ICO. Any breach of unencrypted special data must be reported to the ICO regardless of the risk that it is considered to present to the rights and freedoms of the data subjects.

During office hours the report will usually be done using the ICO's DPA security breaches helpline [0303 123 1113, option 3]

Out of office hours the report will be made using the ICO's security breach notification form (link below) and emailed to casework@ico.org.uk

https://ico.org.uk/media/for-organisations/documents/2666/security_breach_notification_form.doc

7.5.3 *Our response to a data breach*

In the event of a data breach the DPO, or other member of SMT, will:

i) Undertake a risk assessment of the potential damage arising from the identified breach;
ii) Notify the data subjects concerned, as soon as reasonably possible, if there is considered to be a significant risk to their rights and freedoms, offering advice as to how the individual might protect themselves, where appropriate, and setting out how the Settlement is responding;

iii) Take all reasonable steps to prevent the breach re-occurring;
iv) Take all reasonable steps to recover and/or correct the data that has been breached.

7.6 DP by design and DP impact assessments

7.6.1 DP by design is the commitment to make DP considerations an integral part of any organisational activity that might have implications for the way that personal data is processed. For example, a project to develop a new IT system or the introduction of a new service would have DP issues addressed throughout the course of the project, rather than an after-thought at the end. The Settlement has agreed to this commitment in order to help ensure that it continues to meet its obligations under GDPR and any future changes to DP legislation.

7.6.2 One of the key tools for ensuring that DP is built in to the culture of the Settlement will be the use of DP Impact Assessments (DPIA). These are, in effect, risk assessments on the potential impact on DP of the change(s) being considered.

8. Meeting our obligations under the Freedom of Information Act (2000)

8.1 The Freedom of Information Act was introduced so that government, and a wide range of public bodies, should become more open and transparent.

8.2 For all organisations covered by the Act, including publically funded colleges such as the Settlement, it introduced a presumption that anyone asking for information should be given it. The person making the request does not have to provide any justification for the request and the person to whom the request is made has to justify its refusal.

8.3 Information can also include associated information, such as the date of a document, when it was reviewed and who its author was.

8.4 The Settlement publishes a considerable amount of information, much of it on its web-sites. One of the ways of meeting the requirements of the FoI Act is through the Settlement's publication scheme.

8.5 Handling an FoI request

8.5.1 All requests should be forwarded to the Data Protection Officer (DPO) as soon as possible. Requests must be in writing but this includes in electronic form such as emails. The requestor must state their proper name, give an address for correspondence and explain what information is being requested.

8.5.2 If the request is incomplete and/or unclear the DPO will seek clarification from the requestor.

8.5.3 All accepted FoI requests will be logged by the DPO.

8.5.4 All requests will be responded to within 20 days. If a full and final response is not possible then a holding letter will be sent explaining the reason for the delay.

8.5.5 A FoI request may be turned down on any of the following grounds:

- It will cost too much in staff time to produce the information (over £450 based on staff cost of £25 per hour)
- The request is considered vexatious
- The request is a repeat of recent request
- The information requested is personal in nature (as defined by the DPA)
- On public interest grounds (requires justification)
- Prejudicial to the conduct of public affairs (requires justification)
- Where information has been received in confidence (requires justification)
- Where disclosure would be subject to legal action by a third party
- If reasonably accessible elsewhere
- Prejudicial to commercial interest (requires justification)
- Prohibited by law

8.5.6 In some limited cases even the disclosure of the holding of the information may be problematic. In such a case, the Settlement has the right to issue a 'neither confirm or deny' statement.

8.5.7 If the response to an FoI request is a refusal to provide some, or all, of the information requested, then an explanation of the grounds for the refusal should be clearly given. Any response offering less than full disclosure should offer the person making the request the opportunity to ask for the decision to be reviewed.

8.5.8 Ultimately, if after review, the request is still refused, either in whole or in part, then the person making the request should be advised of their right to complain about the decision, within 10 working days of their receipt of it. In the first instance this would be to the Warden and would need to be in writing, with a clear explanation of why the person making the request disagrees with the explanation given by the DC.

8.5.9 The Warden will provide a written response within 20 days of receipt of the complaint.

8.5.10 If the person making the request remains unhappy with the outcome of their complaint to the Warden they should be advised to write to the Information Commissioner's Office.

9. The Settlement's Publication Scheme

9.1 The Settlement publishes a number of documents under its Publication Scheme on its web-site. This includes, as a minimum, the following:

- The Settlement's Values and Mission
- Student and Client charters
- Names of and basic information about trustees
- recent Board minutes
- a clear explanation of the legal advice that can be provided
- Equality data
- Signed accounts
- the current strategic plan
- reports (Ofsted, Education Centre self-assessment, impact, Widening participation)

- Key policies
- Our complaints procedure

10. Use of CCTV

10.1 The Settlement uses CCTV for the purpose of the detection and prevention of crime.

10.2 The use of CCTV, and the legitimate purpose for its use, is widely advertised in the parts of the building where it is in use. The system is used overtly and there is no attempt to conceal its usage.

11. Records Management

11.1 The main aims of records management are as follows:

- To protect the interests of the Settlement, its staff, students, clients and stakeholders through the maintenance of high quality information
- To comply with statutory and regulatory requirements
- To ensure accessibility where appropriate but also sufficient security to prevent unauthorised access;
- To support decision making across the Settlement
- To provide evidence in any cases of litigation

11.2 The responsibilities and rights of all staff relating to the collection, retention and use of records will be regularly communicated to all staff and will be part of the induction programme for all new staff.

11.3 This policy will be available to all students and clients through the respective web-sites of the Adult Education and Legal Centres.

11.4 The minimum periods of retention of different types of records is set out in Appendix F.

11.5 General guidance on records management

11.5.1 Records should be completed as soon as possible after the event to which they refer.

11.5.2 Records should be, as far as it is reasonably possible to make them, complete, authentic, reliable and in a usable format.

11.5.3 All records should have an identifiable owner.

11.5.4 Although the Settlement does not have a centralised document naming protocol, each record manager should endeavour to use a name that assists with the identification of the content without necessarily having to review the content.

11.5.5 All records should be stored in such a way as to enable appropriate access. This includes a required level of security where records contain anything other than publically available information.

11.5.6 Paper records in regular use should be kept near to the principal user, as far as this is practically possible. Infrequently accessed records should be centrally stored or stored off-site if necessary.

11.5.7 Except in exceptional circumstances all records should be immediately accessible by more than one member of staff.

11.5.8 Emails, and other electronic files, are just as capable of being records as those held on paper. All of the principles and practical management guidance should be applied equally to electronic records as they are to paper records.

11.6 Archiving

11.6.1 Records should be stored in such a way as to make the relevant retention periods easily identifiable. Archiving boxes should also be marked with the date of archiving and references, along with the required date of destruction.

11.6.2 Records should be stored in such a way as to enable appropriate access. Boxes should not be overfilled.

11.6.3 Boxes containing personal data or other confidential material should be marked as such. Any restrictions on who can access the records should also be clearly marked.

11.6.4 Each centre should have its own archive retrieval policy, with appropriate security in built, aimed at ensuring that no unauthorised person has access to records they are not entitled to see.

11.7 Disposal

11.7.1 All physical records will be disposed of using an appropriate service provider with a certifiable document disposal process.

11.7.2 All electronic records to be disposed of will be erased in such a way as to minimise the risk of them being reconstructed.

Glossary of terms

General Data Protection Regulations (referred to as GDPR)	The rules that update the original 1988 Data Protection legislation, effective 25 May 2018.
Personal data	Any information that refers to an identifiable, living person that is held in a structured format.
Special data	Particular personal data for example information about race or ethnicity (see Appendix C for full list).
Data subject	An individual to which the data refers.
Data Controller/Owner	The person responsible for managing the data.
Data Processor	A person or organisation responsible for processing data.
Data Protection Officer	The person in the organisation who has the overall day to day responsibility for the management of personal data.
Processing data	The organisation, adaption or alteration of data. The retrieval of, consultation with or use of data. The disclosure or dissemination of data. The alignment, combination and/or erasure of data.
Privacy notice	The statement made by the Data Controller to the Data Subject explaining that their personal data is being held and all of the relevant information about this that they have the right to know.
Subject Access Request	A request made by a Data Subject to be given copies of all of their personal data held and certain information about its use.
Data Protection Impact Assessment	This is a risk assessment of the likely impact on personal data from any changes, such as changes to processes, adopting new technology or the introduction of a new activity.

Data breach	When a security incident occurs that affects the confidentiality, integrity or availability of personal data.
Data Protection by design	This is the commitment to always consider the impact on DP whenever a policy or process is amended.

The Data Protection General Principles under GDPR

The following principles apply to the processing of all personal and special data:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) 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;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) 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;

e) 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; and

f) 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."

[Note – The above is taken directly from the ICO website]

What is 'special' personal data?

Special personal data is personal data that refers to data in one, or more, of the following categories:

(a) Racial and/or ethnic origin;

(b) Political opinions;

(c) Religious or other beliefs of a similar nature;

(d) Membership of a trade union;

(e) Physical or mental health or condition;

(f) Sexual life;

(g) The commission of or alleged commission, of, any criminal offence; or

(h) Proceedings related to the commission, or alleged commission, of,any criminal offence, the outcome of such proceedings or the sentence of any court in such proceedings.

There are additional criteria that apply when considering the processing of special data. (See Appendix D)

The legal basis for holding personal data

For each type of personal data held there must be one of the following legitimate legal basis for processing that data:

- Consent of the data subject
- Processing is necessary for the performance of a contract with the data subject (or to take steps to enter in to a contract with the data subject)
- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of the data subject (or another person)
- Processing is necessary to fulfil the legitimate purposes of the data controller (or a third party), except where such interests are overridden by the interests, rights or freedoms of the data subject

*For each type of **special** personal data held there must be one of the following legitimate legal basis for processing that data:*

- Explicit consent of the data subject (unless reliance is prohibited by law)
- Processing is necessary for carrying out obligations under employment, social security or social protection law or a collective agreement
- Processing is necessary to protect the vital interests of the data subject (or another) where the individual physically/legally cannot give consent
- Processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim, providing that the processing relates only to members (or former members or those who have regular contact with it in connection with its purposes) and provided that there is no disclosure to a third party without consent
- Processing relates to data clearly made public by the data subject
- Processing is related to a legal claim or where courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest based in law which is proportionate to the aim pursued and which contain appropriate safeguards
- Processing is necessary of preventative or occupational medicine; for assessing the working capacity of an employee; medical diagnosis; the provision of health or social care treatment (or the management of lawful health or social care systems; or a contract with a health professional
- Processing is necessary for reasons of public health
- Processing is necessary for archiving in the public interest, or scientific and historical research or for statistical purposes (as defined by Article 89(1))

Appendix E

What we need to tell data subjects in our privacy notices

The requirements are set out in the table below:

Information to be supplied	When data obtained directly	When data obtained indirectly
Identity and contact details of the data controller and the DP Officer	✓	✓
Purpose of the processing and the lawful basis for it	✓	✓
The legitimate interests of the data controller	✓	✓
Categories of personal data		✓
Recipients of personal data	✓	✓
Details of transfers to third countries and safeguards	✓	✓
Retention period or criteria used to determine retention	✓	✓
The existence of the data subject's rights	✓	✓
The right to withdraw consent at any time (where relevant)	✓	✓
The right to lodge a complaint with the ICO	✓	✓
The source of the data and whether the source was publically accessible		✓
Whether the personal data is part of a statutory or contractual requirement and what the consequences of failing to provide the data might be	✓	
The existence of automated decision making processes	✓	✓

Appendix F

Retention of records

This table sets out minimum periods we will keep records (whether paper or electronic)

Type of record	Minimum retention period	Other information
Personnel files including documentation of grievance and disciplinary processes	6 years from the end of the individual's employment [Basic details - name, DOB and dates employed for 20 years]	Commitment to provide employment references and in case of litigation
Details of trustees	6 years after they cease to be trustees	
All information relating to redundancies involving less than 20 staff	6 years from the date of the redundancy	
All information relating to redundancies involving more than 20 staff	12 years from the date of the redundancy	
All records relating to maternity, paternity, adoption and parental leave pay	3 years from the end of the tax year they relate to	
Governance and constitutional documentation	12 years from any change in the documentation or from the point in time that the document is superseded	
Client legal files (incl. client complaints)	7 years after the closure of the case. For any client under 18 years of age it should be kept until the client reaches the age of 25.	To be in a position to respond to any further legal action
Client enquiry forms	18 months (unless a full client file open in which case it is kept as part of that file)	
Student records including academic achievement and performance	10 years [Basic details - name, DOB, courses attended and achievements for 20 years]	To be able to provide academic references
Student application forms	1 year	To be able to deal with any challenge from a student
All primary financial documentation including payroll information, invoices, signed accounts	6 years	Includes financial claims to the SFA

Type of record	Minimum retention period	Other information
Contracts	6 years from the end of the contract	
Returns to financial authorities (HMRC and pension providers)	3 years	
Returns to non financial public bodies (such as the SFA)	3 years	
Property interests	12 years from the time of disposing of the property	Includes any secured loans or mortgages
Policies	6 years from the amendment of the policy or the point in time when it is superseded	
Application forms and selection process documentation	1 year	To be able to respond to any challenge to the recruitment/selection and appointment process
All documentation relating to accidents	3 years from the date of the last reported incident	
All Health & Safety compliance records	Until superseded by later records	
Reports from external bodies specifically regarding any aspect of the Settlement's activities	6 years (longer in specific instances)	This does not include reports of general interest that have not been compiled specifically about the Settlement
Health records (general)	During employment only	
Health records relating to the termination of employment	3 years	To be able to respond to any legal action
Governance documents including those outlining constitutional matters as well as minutes and resolutions	Permanently or 6 years after they have been superseded	

Note - The above minimums will be extended in the event of any specific requirements instituted by the approved authorities or where the Settlement enters in to any contractual arrangement where a longer retention period for documentation is specified.