Partnership Agreement

between

_____ (Commissioner)

and

_____ (Provider(s)

1. INTRODUCTION

This section should contain an initial outline of the purpose of the Agreement. This should specify the lead organisation and the reasons for partnership.

2. PLANNING

This section should contain a description of how planning will be managed. This may include the sharing of prior learning, targets and Individual Learning Plans, in the case of local partnerships. In an agreement between the LA and providers, this may include projected numbers, qualification routes and projected outcomes and destinations.

The information required prior to the start of the Agreement, and timescales, should be specified, as should the methods of transfer and the named contact to whom information should be sent.

2.1 Planning Detail

-
-

3. RESPONSIBILITIES

3.1 Lead Organisation:

This section should outline senior and strategic responsibilities as well as responsibility for co-ordination, operational management and quality assurance.

3.2 Partner(s):

As above.

Relevant personnel should be named (in Appendix B) together with up-to-date contact details, on the understanding that this list may change with circumstances and that relevant parties will be informed of any changes together with new names, in advance wherever possible.

3.3 Specific Responsibilities:

This should outline the detailed responsibilities of all those listed above. This may include regular meetings, responsibility for convening meetings, effective co-ordination, information sharing, day to day operations, quality of teaching and learning, target setting and review, curriculum content, assessment requirements and arrangements, management of learners (including absence and punctuality, progress reporting etc.), learner performance, and timetabling arrangements

4. COMMUNICATION AND INFORMATION / DATA SHARING

This section should specify communication strategies and any required sharing of data and information between partners. In such instances the Agreement should specifically address data management and protection issues. A data sharing protocol is a formal agreement between organisations that are sharing personal data. It explains why data is being shared and sets out the principles and commitments organisations will adopt when they collect, store and disclose personal information about members of the public.
An outline of areas to be covered is given below:

4.1 List of Partners to the agreement

Who are the intended Partners to this Agreement and what are their responsibilities? This should be covered in sections 1-3 above. Within the protocol, formally establish who will collect, store and disclose personal information. Show that all the organisations are committed to maintaining agreed standards on handling information, by publishing a list of senior signatories with the Agreement.

Do not forget to define the responsibilities of any sub-contractors within the protocol, as they will also be subject to the agreed standards.

Consent and the Data Protection Act 1998

A common approach on the issue of consent should have already been decided. If consent is required to enable the collection, or disclosure of information, it has to be informed, specific and fair. All of the partners will have to agree procedures for obtaining consent within the law.

The protocol/agreement should mention that when obtaining consent, the data subject must be informed of the purpose for which the information is being collected, how it will be used and with whom it will be shared. Also state that if consent is sought and refused, objections must be recorded appropriately and each organisation must abide by the refusal.

4.2 Information to be shared

What is the specific business need/objective for information sharing? Elements of the procedures for sharing data need to be outlined briefly within the Agreement. Each organisation should also describe them in detail within their own codes of practice and management guidance. Consider:

Anonymised and Aggregated Data

Anonymised data are individual data records from which the personally identifiable fields have been removed. Aggregated data are data which are processed to produce a generalised result, and from which individuals cannot be identified. This might include data brought together to give a broad understanding of e.g., ethnicity distribution.

Personal Data

Personal data are defined as data which relate to a living individual who can be identified and includes any expression of opinion about the individual
Such personal data might include, but not be limited to:

- Name
- Address

- Telephone number
- Date of birth/age
- Case history
- A unique reference number if that number can be linked to other information which identifies the data subject.

The individual who is the subject of the data has the right to know who holds their data and how such data are or will be processed, including how such data are to be shared.

Sensitive Data

Certain types of data are referred to as “sensitive personal data”. These are data which relate to the data subject’s:

- Racial or ethnic origin
- Political opinions
- Religious beliefs, or other beliefs of a similar nature
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence
- Any proceedings for any offence committed, or alleged to have been committed.

4.3 Data Control

Any organisation which “determines the purposes for which and manner in which any personal data are, or are to be, processed” is called a “data controller”.

At all times, when providing data to partners, the partner responsible for delivering a service will be considered to be the data controller, as opposed to the partner who may be the first point of contact.

This will include:

- appropriate technological security measures, having regard to the state of technology available and the cost of implementing such technology, and the nature of the data being protected
- secure physical storage and management of non-electronic data
- password protected computer systems
- restricted access to data and taking reasonable steps to ensure the reliability
- of employees who have access to sensitive data
- ensuring data is only held as long as is necessary, in line with Data Protection principles
- appropriate security on external routes into the organisation, for example Internet firewalls and secure dial-in facilities.

Partners are themselves responsible for complying with security irrespective of the specific terms of this agreement.

If there is a requirement to supply data to any external body, full records will be kept of when data is supplied to external and other governmental organisations.

4.4 Complaints

Complaints about personal or sensitive information held by the partnership must be made in writing to the person or organisation holding this information, detailing the reasons for the complaint.

4.5 External organisations

Sensitive and personal data are not passed to organisations, except where an organisation may have a legal and legitimate reason for access and a requirement for the data in order to carry out its function.

Organisations wishing to have access to named data must first sign up to the lead organisation's data sharing agreement for personal and sensitive data, submit a request as to which data elements are required and justify their request for access.

This request will then be considered, and access to the data either granted or denied.

Personal and sensitive data are not shared unless the need is totally justified.

4.6 Changes to Agreements

This agreement will be reviewed periodically and consequently it may be subject to change. This agreement will be available on-line and in the public domain. On changing an agreement, the new publication will be provided on the partner web sites.

5. PURPOSE OF INFORMATION SHARING

What specific information is required for the purpose of this agreement?
Include an explanation of how anonymised information may be used where appropriate.

A written protocol should start by explaining the reasons for sharing personal information. It should also state whether partners are obliged to, or are merely enabled to, share data. Where it is relevant to do so, achievement targets should be set. (For example, a data sharing initiative may aim to provide effective service improvements that are measurable).

The purpose of the data sharing arrangement must be approved, understood and formally agreed by those entering into a data sharing agreement.

In instances where organisations develop a database to share pooled data, it is necessary to establish which organisation will act as the 'data controller' - they alone will have responsibility for disclosing information on a need to know basis.

The data controller will be responsible for storing the information safely by limiting access. Reduce the risk of information being seen by an unauthorised person by establishing levels of access. State within the protocol, whether the organisations will be anonymising aggregated information on the database, or pseudonymising data where only a few authorised personnel can access the information with a 'key' (sometimes this is required by legislation).

Remember that when disclosing data to a third party, the database is still subject to rules of confidentiality. Such databases must contain relevant information and the way that information is used should not exceed the protocol's original purpose.

6. BASIS FOR INFORMATION SHARING

What are the specific lawful powers/obligations for the processing of information? What considerations apply to make the processing fair under the terms of the Data Protection Act 1998? Please also state which conditions of Schedule 2 and Schedule 3 are relevant to this sharing (An outline of conditions is given in Appendix 1).

7. EXCHANGE OF INFORMATION

State explicitly how and what information is to be shared, consider methods such as encrypted email, mail, fax and how regularly these are to take place e.g. initially, weekly, termly, summatively.

8. TERMS OF USE OF THE INFORMATION.

Add a clear statement of how the information is intended to be used and any restrictions which may apply.

9. DATA QUALITY ASSURANCE.

Explain what standards will apply for data quality and how errors will be handled.

10. DATA RETENTION, REVIEW AND DISPOSAL

Explain how long the information is intended to be retained for the purpose and any specific review or disposal arrangements that apply.

11. ACCESS AND SECURITY

Explain the standards and conditions which are required to protect the information concerned. Include any special arrangements which might apply. For example, access to files will be restricted, operate a clear desk policy, employees given access on a need to know basis. Organisations should agree the position on subject access rights to the information being shared, and be clear on any limits on people's access to their personal information.

12. GENERAL OPERATIONAL GUIDANCE

Include or reference any general operational guidance which is relevant to the purpose of the agreement that is not covered in any other section. Details of relevant contacts can be appended to the document.

13. MANAGEMENT OF THE AGREEMENT

Additional information should be provided to address the following.

- Handling of complaints or breaches of the agreement
  State that there is a commitment to establishing a system to deal with complaints about the way that organisations handle information. Organisations will need to appreciate that there will be differences in the complaints procedures of other partners. A Foundation Learning Consultative or Steering Group could help to establish some consistencies and standards across the board. These procedures do not need to be detailed in the protocol, but it is helpful to mention the following in the document:

- Complaints about the use, or disclosure, of personal information must be addressed by the organisation where the complaint originated. If the complaint affects more than one partner organisation, it should be brought to the attention

of the appropriate Data Protection officer/s and these officers should liaise with their opposite numbers to investigate the case.

- Recognise the possibility that the protocol could be breached and state that organisations will have to investigate improper use of personal information. Organisations will find that a good audit trail will prove to be invaluable in these circumstances. Breaches will need to be recorded, investigated and the findings noted. It should then be brought to the attention of a senior member of staff. Initially partners may not be clear about what constitutes a breach and examples should be made available, as and when they occur.

- Each partner (if not covered by Crown Indemnity) should strongly consider having indemnities for claims, losses, liability or costs suffered as a consequence of any information being wrongly disclosed, or as a result of any negligent act, or omission by any other partner.

- Handling of requests for information under Data Protection/Freedom of Information

- Appropriate Signatories

- Review of the Agreement
  The protocol should be reviewed and it is helpful to say when this will take place. Initially the Steering Group may want to do this after 3 and/or 6 months, and then annually. If operational problems and complaints arise on a regular basis, the document may need to be amended. If these changes are substantial, the document will need to be reviewed completely.

- Compliance with the Agreement

- **Building awareness - Training**
  The success of the protocol will depend upon visible high level support from senior managers within each organisation. State that there is a commitment to raising awareness of the protocol through training. Each organisation should ensure that appropriate officers/professionals are sufficiently trained to make lawful decisions about data sharing. It may be useful to arrange joint-training sessions to allow people from the different organisations to meet each other, to build co-operation between partners, and to promote a better understanding of the objectives of the data sharing arrangement.

  At an operational level, staff should be made aware of procedures. A staff booklet and a checklist for disclosing data and obtaining consent should help maintain a level of consistency and confidence that the correct procedures are being followed.

- Closure/termination of agreement

- Indemnity

14. TIMETABLE – where this Agreement is between delivery partners.

The exact annual and weekly timetable structure of each individual programme will be agreed between providers in advance of the start date of the programme, normally during the preceding term. All programmes will be delivered according to agreed criteria for cost-effectiveness, availability of resources, and learner welfare.

15. QUALITY ASSURANCE

Outline any quality assurance arrangements from all partners. How will quality be assured? This may include site visits, scrutiny of records and/or observations.

15.1 Inspection

a. When Ofsted informs any partner of a forthcoming inspection:
   1 The organisational lead will need to inform all partners as soon as possible so that relevant information and data can be collated
   2 The organisational lead will also need to establish as soon as possible whether collaborative provision will be a focus of that inspection.

b. If the provision is to be inspected, the organisational lead must inform the lead inspector that a letter must be sent to delivery partners, clearly stating:
   1 when the inspection will occur
   2 who the Lead Inspector will be
   3 when he/she will make contact with the other providers to arrange the visit

d. Once providers are informed, relevant leads will ensure managers and staff are briefed and will liaise with the Inspector to:
   1 prepare an inspection schedule of lessons to be seen
   2 agree discussion and feedback times

e. After the inspection, outcomes will be shared and a post-inspection action plan agreed

16. FEES

An outline of any associated Fees, or costs should be provided here. In some instances this may be based on sharing for mutual benefit, rather than any financial agreement.

Fees and/or arrangements should consider costs of:

- Teaching staff
- Essential physical resources including relevant equipment, protective clothing, and consumables
- Exam registration and administration fees, except wherein registration is late.
- Fares and entrance fees to any off site visits or events that form part of the programme.

17. INVOICING

This should state the timescale for invoicing and payment in accordance with financial regulations.

Queries relating to invoiced should be raised immediately with a named person.

SIGNATURES

I understand and agree to the above items.

For and on behalf of lead organisation:

_____

Signed: _____ Date: _____
(Strategic lead or designated senior representative)

Print name and position:

_____

For and on behalf of the partner provider:

_____

Signed: _____ Date: _____
(Strategic lead or designated senior representative)

Print name and position

Please sign and return to (named person)

Appendix 1

ROLES AND RESPONSIBILITIES FOR THE MANAGEMENT AND DELIVERY OF COLLABORATIVE PROVISION, INCLUDING ADMINISTRATION

Example Only

Providers could be FE colleges, work-based learning providers or other independent alternative providers

ESCs – Education Support Centres

Phase	Responsibility
PRE-ENTRY	
Learners will be selected based on the agreed criteria for the programme.	School/ESC/ Provider
Schools/ESCs will provide a named co-ordinator	School/ESC
School/ESC will organise information meetings for parents with contributions from the college/WBL/alternative provider to ensure all learners are clear about the programme offer and are given fair, equal and impartial advice and access to different learning opportunities. The college/WBL or alternative provider will ensure appropriate staff attend these meetings.	School/ESC/ Provider
Schools/ESCs will seek consent from parents for learners to attend the programme and for the learner's personal details to be passed on to the provider.	School/ESC
The school/ESC will provide the provider with details of the learners prior to starting the programme to include, personal details, targets, any health issues the provider should be aware of, learning needs/difficulties, behavioural problems and emergency contact numbers.	School/ESC School/ESC
Schools/ESCs will provide adequate transportation arrangements ensuring learners arrive on time	

ON PROGRAMME	
Learners will come to the provider at an agreed time (in the case of a college this will be confirmed by individual areas), to collect all relevant information eg for a college to enrol and collect passes, handbooks and timetables. Procedures will be explained and contracts issued if appropriate.	Provider
Programme Leaders (Programme Lecturers/Personal Tutors) will be responsible for the day to day running of the programme in their own individual areas, reporting to the Manager/Course Co-ordinator regularly as appropriate to the institution. Should an issues arise that cannot be dealt with by the 'tutor', the Manager/Course Co-ordinator will be contacted immediately.	Provider Schools/ESCs
HEALTH & SAFETY	
Providers will ensure that all learners are appropriately equipped and inducted to meet the Health & Safety requirements of the area that they will be working in.	Provider
The provider will provide protective clothing for the programmes eg vocational areas. The schools/ESCs will ensure that learners are appropriately dressed for the provision.	Providers/ESCs /Schools
Risk assessments will be undertaken for each area in which 14-19 learners will be working. Copies of these assessments will be made available for schools and parents as requested. For alternative providers this will form part of the annual check by the Health and Safety Team Manager (Education) of HCC	Providers/ Schools/ESCs
Schools will inform providers of any particular needs of the learners with regard to health and safety.	Schools/ESCs
Should an accident occur, the provider will take appropriate action and the school/ESC and parents informed. If emergency hospital treatment is required the provider will call an ambulance and escort the learner until such time as a parent, guardian or school representative arrives.	Provider
For insurance purposes, the provider will ensure that the Employers' Liability Insurance is adequate to cover under 18s in the 'trainee/employee' role. This insurance does not cover travel to and from the provider.	Provider
The programme leader/tutor is responsible for the supervision and safety of learners during the session contact time	Provider
All staff are CRB checked.	Provider

ATTENDANCE & PUNCTUALITY	
Learners will be expected to attend at all times. Providers will register the learners' attendance at each session.	Provider
The provider will inform the school/ESCs/parents and learners of the minimum requirement in attendance to ensure success on the programme.	Provider
In the event of learners falling sick whilst with a provider the school/ESC will be notified immediately by the provider and will make contact with parents (if agreed in the contract).	Provider
BEHAVIOUR	
The usual provider rules apply regarding learner behaviour in and around the site of the provision. The learners may be issued with a programme agreement and may also be required to follow additional rules for their particular provider or programme.	Provider
Where a learner cannot behave appropriately they will be withdrawn from the provision and returned to ESC/school. The Manager/Course co-ordinator will inform the school, and parents if agreed where possible.	Provider
If behaviour of a learner continues to cause concern then the school/ESC and provider together will decide on an appropriate programme of action and notify parents/carers/purchasers. The provider, in consultation with the home institution, reserves the right to withdraw a learner from the programme.	School/ESC/ Provider
DISCIPLINARY PROCEDURES	
Whilst 14-19 learners are on provider premises, they will be subject to the provider's disciplinary procedures. However, the provider would look to the home school to take forward any disciplinary process.	Provider/School

PROGRESS MONITORING	
Reports on the attendance, progress and performance of learners will be sent to schools/ESCs on a termly basis by the programme leader.	Provider
The provider may hold open evenings for parents/carers on the site of the provision to meet with staff.	Provider
The school/ESC will invite training/teaching staff to attend school based parents' meetings where appropriate. Providers should also be invited to make contributions to learner review reports and meetings (if appropriate and part of the purchase agreement).	Provider
SUPPORT FOR LEARNERS	
Where learners are entitled to dedicated individual learning support in school/ESC this should follow them into the provider and a school/ESC employed LSA attend with the learner.	School/ESC
The school/ESC will timetable a member of staff to visit the learners at the provision, at an agreed point during the programme	School/ESC
OFF SITE WORK	
If learners are to attend visits off provider premises as part of the programme, programme leaders/tutors will complete an external activities risk assessment form and inform the school/ESC in advance.	Provider
Permission for off site work, visits or events will be sought in writing from parents and a copy of all letters forwarded to the provider.	Provider
The school will inform the provider in advance of any school based visits, events or exams that might affect attendance.	Provider
WELFARE OF LEARNERS	
The provider will inform the school immediately of any concerns regarding the welfare of learners. If an emergency arises regarding a learner's care the school's/ESC's Child Protection Officer should be notified immediately. If college based, learners can make use of the college Guidance team and/or Connexions Personal Advisers.	Provider

PROGRESSION & EXIT	
End of year/programme summative reports will be sent to the school/ESC and certificates (if appropriate) should be awarded to all programme completers.	Provider
The school/ESC will notify immediately the programme leader/tutor of any learner who has withdrawn from the programme.	School/ESC
The school/ESC and provider will work together to collect information about the achievement and progression of learners.	School/ESC/ Provider

CONTACT DETAILS

Programme Leader/Course co-ordinator:

Email, tel., mobile and address…….

School/ESC-based Contact (or Purchaser)

Email, tel., mobile and address…….

Manager:

Email, tel., mobile and address…….

School/ESC Head Teacher

Email, tel., mobile and address…….

Appendix 2
This section would need to be completed in line with County Policy

Complaints System

- **WHAT IS A COMPLAINT?**
- **WHAT IS THE PROCEDURE FOR COMPLAINTS?**
- **WHAT WILL HAPPEN IN RESPONSE TO YOUR COMPLAINT?**
- **WHAT DO YOU DO IF YOU ARE NOT SATISFIED WITH THE OUTCOME?**
- **WHAT IF YOU WANT YOUR COMPLAINT KEPT CONFIDENTIAL?**
- **WILL ANY RECORD OF THE COMPLAINT BE KEPT OR GIVEN TO ANYONE ELSE?**
- **CAN YOU OBTAIN HELP IN MAKING YOUR COMPLAINT?**

Appendix 3

The legal framework

The Data Protection Act 1998

The Act governs the protection and use of personal data. Personal data means data relating to living individuals.

Any organisation processing (obtaining, holding, using, disclosing and disposing) data is a 'Data Controller' responsible for abiding by the 8 data protection principles and notifying the Information Commissioner of that processing.

The Act gives seven rights to individuals in respect of their own personal data:

1. Right of subject access;
2. Right to prevent processing likely to cause damage or distress;
3. Right to prevent processing for the purposes of direct marketing;
4. Rights in relation to automated decision taking;
5. Right to take action for compensation if the individual suffers damage or damage and distress (as a result of any breach of the act);
6. Right to take action to rectify, block, erase or destroy inaccurate data;
7. Right to request the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

The 8 key principles of the Act are: Principle 1	Personal data shall be processed fairly and lawfully and shall not be processed unless at least 1 of the conditions in Schedule 2 is met and for 'sensitive personal data' at least 1 of the conditions in Schedule 3 is also met.
Principle 2	Personal data shall be obtained for specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose/purposes.
Principle 3	Personal data shall be adequate, relevant and not excessive in relation to the purpose/purposes for which they are processed.
Principle 4	Personal Data shall be accurate and, where necessary kept up to date
Principle 5	Personal data shall not be kept for longer than is necessary for that purpose/purposes.
Principle 6	Personal data shall be processed in accordance with the rights of the data subject under this Act.
Principle 7	Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage to personal data.
Principle 8	Personal data shall not be transferred to a country or territory outside the EEA without an adequate level of protection for the rights and freedoms of the data subject in relation to the processing of personal data.

Schedule 2 and Schedule 3 conditions

Lawful processing of personal data requires that one condition in Schedule 2 should be met; and in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met. **Conditions in Schedule 2**	
Paragraph 1	The data subject has given consent to the processing.
Paragraph 2	The processing is necessary for (a) the performance of any contract to which the data subject is a party; (b) for the taking of steps at the request of the data subject with a view to entering into a contract.
Paragraph 3	The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
Paragraph 4	The processing is necessary in order to protect the vital interests of the data subject.
Paragraph 5	The processing is necessary: (a) for the administration of justice; (b) for the exercise of any functions conferred on any person by or under any enactment; (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department; or (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.
Paragraph 6	(1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject. (2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Appendix B: the legal framework **Conditions in Schedule 3**	
Paragraph 1	The data subject has given explicit consent to the processing.
Paragraph 2	The processing is necessary for the purposes of exercising or performing a legal right or obligation in the context of employment.
Paragraph 3	The processing is necessary to protect the vital interests of the data subject or another in cases where consent cannot be obtained.
Paragraph 4	The processing is of political, philosophical, religious or trade union data in connection with its legitimate interests by any non-profit bodies.
Paragraph 5	The processing is of information made public as a result of steps deliberately taken by the data subject.
Paragraph 6	The processing is necessary in connection with legal proceedings or the seeking of legal advice.
Paragraph 7	The processing is necessary: (a) for the administration of justice; (b) for the exercise of any function conferred on any person by or under any enactment; (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.
Paragraph 8	The processing is necessary for medical purposes and is carried out by medical professionals or others owing an obligation of confidence to the data subject.
Paragraph 9	The processing is necessary for ethnic monitoring purposes.
Paragraph 10	The personal data are processed in circumstances specified in an order made by the Secretary of State for certain purposes. The Data Protection (Processing of Personal Data) Order 2000 (SI 2000 No 417) specifies a number of circumstances in which sensitive personal data may be processed such as crime prevention, policing and regulatory functions (subject to a substantial public interest test); insurance, equality monitoring in the area of disability and religious or other beliefs; and research. A further order relates to the processing of sensitive personal data by MPs and other elected representatives (The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002 (SI 2002 2905)).

The Human Rights Act 1998

The Human Rights Act 1998 incorporates into our domestic law certain articles of the European Convention on Human Rights (ECHR). The Act places a legal obligation on all Public Authorities to act in a manner compatible with the Convention. Should a Public Authority fail to do this then it may be the subject of legal action. The sharing of information between agencies has the potential to infringe Article 8.1 in particular.

Article 8.1 provides that “everyone has the right to respect for his private and family life, his home and his correspondence”. This right may be only breached by a public authority if the breach is in accordance with the law and is necessary in the interest of one of the following legitimate aims: national security, public safety or the economic well-being of the country for the prevention of crime and disorder, for the protection of health and morals or for the protection of the rights and freedoms of others.

The following factors should be taken into account when deciding whether disclosure of information would breach a person's right to privacy

- Is there a legal basis for the action being taken?
- Does it pursue a legitimate aim?
- Is the action taken proportionate and the least intrusive method of achieving that aim?

The Freedom of Information Act (FOIA) 2000

The Freedom of Information Act (FOIA) gives a general right of access to the public of all types of recorded information held by defined public authorities from 1 January 2005.

There are 23 statutory exemptions to the right of access which are either absolute or qualified. Absolute exemptions include personal information if disclosure would breach the data protection principles. Qualified exemptions require the public authority to consider first whether or not the exemption applies, on a case-by-case basis. Secondly, if the exemption does apply, the public authority must then consider whether it is in the public interest to apply the exemption. Further information and guidance can be found at the following web site http://www.informationcommissioner.gov.uk

The Common Law Duty of Confidentiality

This duty arises where information has the necessary quality of privacy. Disclosure of that information without the consent of the individual could give rise to a civil claim for breach of the duty. However it would be a defence to such a claim to show that the breach of confidence was in the public interest and disclosure was to the extent necessary for the performance of a public duty.

Caldicott Principles

The Caldicott Committee carried out a review of the use of patient-identifiable information. It recommended a series of principles that should be applied when considering whether confidential information should be shared. All NHS organisations and Social Services Departments are now required to apply the Caldicott principles. These principles relate to the use of patient-identifiable information and are detailed below. Principle 1	Justify the purpose for using such information. Every proposed use or transfer of such information should be clearly defined and scrutinised and continuing uses reviewed regularly.
Principle 2	Only use such information when absolutely necessary.
Principle 3	Use the minimum information that is required for a given function to be carried out
Principle 4	Access should be on a strict “need to know” basis. Only those staff who need such information in order to carry out their roles should have access and this should be limited to specifically relevant information.
Principle 5	Everyone with access to such information needs to be aware of their responsibilities and their obligations in respect of confidentiality.
Principle 6	Understand and comply with the law. Someone in each organisation that handles personally identifiable information should be responsible for ensuring that the organisation complies with legal requirements.