

Plymouth City Council

Data Protection Policy



City of
Plymouth

Plymouth City Council

Data Protection Policy

Scope:-

This policy must be complied with fully by all Members, Officers Agents and Contractors of Plymouth City Council who collect, hold, process or deal with Personal Data for or on behalf of the City Council.

Plymouth City Council supports the objectives of the Data Protection Act 1998 (the 'DPA') and intends to conform with the requirements of the Act at all times.

1. Processing Personal Data

(for further information please consult the Support to the Data Protection Policy, clause 1)

- 1.1. Personal Data must be processed fairly and lawfully in accordance with the provisions of the DPA.
- 1.2. Personal Data may only be processed for notified purposes as stated within the DPA.
- 1.3. Anyone with responsibility for holding or collecting data must ensure that data kept and processed about any Data Subject is accurate and up to date. All due skill and care must be taken. Data must not be excessive to need and superfluous data must be destroyed or removed from the system.
- 1.4. Directors and Heads of Service are responsible for ensuring compliance with this policy within their departments. Each Director and Head of Service shall nominate a person to ensure compliance with the Act and to ensure that other members of staff are aware of the provisions of the Act. This person shall be called the Data Protection Act Representative. The nomination of such a person shall not release other members of staff from compliance with this Act and this policy.
- 1.5. Any processing of sensitive data must comply with the special and more stringent rules set out in the DPA.

2. Security and Registration

(for further information please consult the Support to the Data Protection Policy, clause 2)

- 2.1. Each Member, Director and Head of Service are responsible for ensuring that data cannot be accessed by unauthorised personnel and to ensure that data cannot be tampered with, lost or damaged. All superfluous data must be disposed of in a secure manner.
- 2.2. The Information Commissioner keeps a register of all organisations, which process data. The Council shall submit a Notification to the Information Commissioner and pay the requisite fee at least once a year. This will be done centrally by the City Treasurer. Directors and Heads of Service must furnish the City Treasurer with any information requested for this purpose. Directors and Heads of Service must notify the City Treasurer immediately if, during the course of any year, this information changes, and the City Treasurer must up date the Register entry accordingly. Members may have to register personally with the Information Commissioner with respect to constituency or party records.

3. Agents, Partner Organisations and Contractors

If a Contractor, Partner Organisation or Agent of the Council is appointed or engaged to collect, hold, process or deal with Personal Data for or on behalf of the Council or if they will do so as part of the Services they are providing to the Council, the Lead Council Officer must as part of evaluation obtain confirmation that the Agent, Partner Organisation or Contractor is able, willing and does comply with the DPA. There must be specific obligations in every such contract requiring the Contractor to comply with the DPA.

4. Disclosure of Personal Data

Personal Data will only be disclosed in accordance with the provisions of the DPA.

5. Access Rights by Individuals

(for further information please consult the Support to the Data Protection Policy, clause 5)

- 5.1 An individual may request a copy of any data held about them, or information about the reasons it is kept and processed and the people to whom it is disclosed. The information must be provided, in clearly understandable terms within 40 days of a valid written request and the payment of the required fee.
- 5.2 A person seeking information shall be required to prove their identity in accordance with the DPA. The 40 days will run from the date the person provides this information, and pays the required fee.
- 5.3. Information may be withheld where the Council is not satisfied that the person requesting information about themselves are who they say they are, or when the requester is an organisation or body where the Council are not satisfied that they have the authority to receive that information.

6. Disclosure to and about Third Parties

(for further information please consult the Support to the Data Protection Policy, clause 6)

Personal Data must not be disclosed about a Third Party except in accordance with the DPA. If it appears absolutely necessary to disclose information about a Third Party to a person requesting data about themselves advice must be sought from the City Solicitor.

7. Inaccurate Data

(for further information please consult the Support to the Data Protection Policy, clause 7)

If an individual complains that the data held about them is wrong, incomplete or inaccurate, the position should be investigated thoroughly including checking with the source of the information. In the meantime a caution should be marked on the person's file that there is a question mark over the accuracy. An individual is entitled to apply to the court for a correcting order and it is obviously preferable to avoid legal proceedings by working with the person to correct the data or allay their concerns.

8. Requests by individuals to stop processing information

(for further information please consult the Support to the Data Protection Policy, clause 8)

- 8.1. If data is properly held for marketing purposes, an individual is entitled to require that this is ceased as soon as possible. Requests must be made in writing but generally all written or oral requests should be heeded as soon as they are made. The cessation must be confirmed in writing.
- 8.2. If data is held for any other purposes, an individual may request that processing ceases if it is causing them unwarranted harm or distress. This does not apply if they have given their consent, if the data is held in connection with a contract with the person, if the Council is fulfilling a legal requirement or if the person's vital interests are being protected. Valid written requests must be heeded within 21 days. The cessation must be confirmed in writing.

9. Complaints

Any complaint or concern expressed by an individual in connection with the DPA must be reported to the City Solicitor immediately in case legal action is taken. The City Solicitor will work with the Department to ensure that there has been no breach of the DPA and, if there has, what action needs to be taken to remedy it.

10. Exemptions

(for further information please consult the Support to the Data Protection Policy, clause 10)

There are a number of purposes which are exempt from certain provisions of the DPA. These purposes are listed in clause 13 of the Data Protection Guidance. If you are in doubt about which purposes are exempt and the scope of the exemption please contact the City Solicitor.

11. Violations of Rules and Procedures

- 11.1. It is the responsibility of all employees to report any suspected breaches of the DPA, or of this policy, to their Head of Service in accordance with the Financial Regulations.
- 11.2. It is the responsibility of all Members to report any suspected breaches of the DPA, or this policy, to the Chief Executive in accordance with the Financial Regulations.
- 11.3. Disciplinary action in accordance with procedures approved by the Council, may be taken against any employee or Member who breaches the DPA, or the requirements of this policy.

12. Further Information and Other Related Policies

- 12.1. If in doubt about any aspect of this policy, contact the City Solicitor.
- 12.2. Other related Policies include the Access to Personal Files Policy and the Disciplinary Policy.
- 12.3. Further information can be found in the Support to the Data Protection Policy pamphlet, which includes Data Protection Guidance.

Plymouth City Council

**Support to the Data Protection Policy
(including Data Protection Guidance)**

Support to the Data Protection Policy

including Data Protection Guidance

1. Processing Personal Data

- 1.1 **'Personal Data'** is defined in s(1) of the DPA as, 'data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller' (the Council is a data controller), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other in respect of the individual.

'Processing' covers a broad range of activities such that virtually any use of personal information or data will amount to processing. (please see the Guidance Section, point 8)

'Processed fairly and lawfully' means that the data must be processed in accordance with the 3 provisions of the DPA. These are the Data Protection Principles, the Rights of the Individual and Notification and Registration. (please see the Guidance Section, points 6 – 12)

- 1.2. **'Notified Purposes'** are the purposes for which the Council is entitled to process that data under its Registration with the Office of the Information Commissioner

- 1.3. **'Data Subject'** is the individual who the data or information is about.

'Data must be accurate and not be excessive to need' which is in accordance with the 3rd and 4th Data Protection Principles. (please see the Guidance Section, point 7)

- 1.5. **'Sensitive Data'** concerns information as to racial or ethnic origin, sexual life, religious beliefs (or similar), physical or mental health/condition, membership of a trade union, political opinions or beliefs, details of proceedings in connection with an offence or an alleged offence)

2. Security and Registration

- 2.2 **'The Information Commissioner'** has responsibility to see that the DPA is complied with. The Office of the Information Commissioner is a government department based in Wilmslow in Cheshire. They can give advise on data protection issues and can enforce measures against individuals or organisations who do not comply with the DPA.

'Notification' the Council's Notification is sent each year by the City Treasurer to the Office of the Information Commissioner it sets out the categories of data subject, the type of information held, the source from which it is obtained, the purpose for which it is held and the people or classes of people to whom it may be disclosed.

3. **Agents, Partner Organisations and Contractors**
<this is intentionally blank>

4. **Disclosure of Personal Data**
<this is intentionally blank>

5. Access Rights by Individuals

- 5.1 When an individual requests a copy of any data that we hold about them, or information about the reasons why information about them is kept and processed etc then we must provide that information within 40 days of a valid written request and the payment of the required fee. The individual should be directed to make their request to the following address:-

Data Protection Officer
Social and Housing Services
c/o Civic Centre
Plymouth
PL1 2EW

The Data Protection Officer will forward the Subject Access Request Form for the individual to complete and return with the required fee of £10.

- 5.3. **'Circumstances in which information may be withheld'** include where the Council is not satisfied that the person requesting information about themselves are who they say they are, or when the requester is an organisation or body where the Council are not satisfied that they have authority to receive that information.

6. Disclosure to and about Third Parties

All references to Third Parties must be removed from the information that is given to the Data Subject, unless the third party gives their consent, or the Council considers it reasonable to provide the information without the other individuals consent.

7. Inaccurate data

It is important that all information that the Council hold about individuals complies with the 4th Data Protection Principle (i.e. that it is accurate and up-to-date.)

8. Requests by individuals to stop processing information

- 8.1 Where the Council receives such a request then we must respond to it within 21 days of receipt, stating whether we have ceased or intend to cease processing the data or stating on what basis we consider the request to be unjustified.

9. **Complaints**
<this is intentionally blank>

10. Exemptions

There are a number of purposes, which are exempt from certain provisions of the DPA. (please see the Guidance Section, point 13)

11. **Violations of Rules and Procedures**
<this is intentionally blank>

12. **Further Information and Other Related Policy**
<this is intentionally blank>

Data Protection Guidance

What is the Data Protection Act 1998 about?

The DPA has been designed so as to ensure that any person who holds, processes, compiles and refers to data about a living individual does so in a way which is both fair to that person and does not cause that person harm.

2. What is Data?

This is defined in s1(1) of the DPA as information which:-

- 2.1. is processed by equipment operating automatically or recorded for that purpose, or
- 2.2. forms part of a 'relevant filing system', or
(a 'relevant filing system' is a set of records that need not be stored on a computer or electronic database but is organised in such a manner that information relating to any individual is readily accessible)
- 2.3. forms an 'accessible record'
(an 'accessible record' is defined in s68 and in Schedules 11 and 12 of the DPA. It covers specific forms of data, including:-
 - (i) a 'health record' containing information about the physical or mental condition of an individual made by a health professional.
 - (ii) an educational record
 - (iii) an 'accessible public record' which includes information held by a local authority for the purpose of any of the local authorities Housing Act tenancies, or social services functions).

3. How does the DPA differ from the old Data Protection Act 1984?

The DPA differs from its predecessor (the Data Protection Act 1984), in that it applies to all information about an individual whether it is held electronically or in a manual filing system. The Act applies to all categories of information, including employment, education and health records, although some types of information are exempt from certain provisions of the DPA.

5. What is Sensitive Personal Data and Non-Sensitive Personal Data?

5.1. Sensitive Data concerns:-

racial or ethnic origin
sexual life
religious beliefs (or similar)
physical or mental health/condition
membership of a Trade Union
political opinions or beliefs
details of/proceedings in connection with an offence or alleged offence

5.2. Non Sensitive Data concerns all other personal data.

4. What is personal data?

Personal Data is defined in s(1) of the DPA as data which relates to a living individual who can be identified:-

from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Personal Data is subdivided into 'Sensitive Personal Data' and 'Non-Sensitive Personal Data'.

6. What are the provisions of the DPA?

The DPA has 3 main provisions, these are:-

- The Data Protection Principles;
- The Rights of the Individual, and;
- Notification and Registration

7. What are the Data Protection Principles?

Anyone who processes Personal Data about a living individual must comply with the following 8 principles:-

- 7.1. To process data fairly and lawfully;
- 7.2. To obtain data only for registered purposes and to process it in a manner which is compatible with those purposes;
- 7.3. To ensure that all data held is adequate, relevant and not excessive in relation to the purpose for which it is held;
- 7.4. To ensure that all data is accurate and up to date;
- 7.5. To ensure that data obtained for a particular purpose is not kept any longer than is necessary for that purpose;
- 7.6. To process data in accordance with the rights of the individual as set out in the DPA;
- 7.7. To ensure that appropriate technical and organisational measures are put into place to protect against unauthorised or unlawful processing of data and against accidental loss, destruction or damage to data;
- 7.8. To ensure that data is not transferred outside the European Economic Area (the European Economic Area is defined as the European Union member states and Norway, Iceland and Liechtenstein) without ensuring that the country to which the data is being transferred has equal data protection measures in place.

8. What does 'processing of data' mean?

This is obtaining, recording or holding data and carrying out any operation or operations on that data including organisation, adaptation, alteration, retrieval, consultation, use, disclosure, alignment, combination, blocking, erasure or destruction'.

The term 'processing' covers a very broad range of activities such that virtually any use of personal information or data will amount to processing.

9. How do we ensure that we process data fairly?

If the data is 'Non Sensitive' then at least 1 of the following conditions must be complied with:-

- 9.1 The individual must give their consent to the data being processed.
(In most cases where data is being processed it would be advisable if possible, to obtain an individual's express consent. Such consent must be 'unambiguous'. Whilst there is not a definition of 'unambiguous' it is likely that it necessitates that consent must be informed, specific, freely given and definitely indicated).
These requirements mean that when an individual is giving data they should be informed of the purpose for which the data is being obtained, the likely recipients of the data and any other specific requirements that it would be fair for them to know (e.g. for what time period the data will be held).

The Council must advise the individual of the following:-

- to whom they are passing the data (e.g. the Council department)
 - the reason why the data is required
 - whether the data will be used for other purposes
 - who the data will be disclosed to (e.g. which other Council departments or outside organisations that the data may be passed to)
 - how they can contact the Council's Data Controller (The City Solicitor)
 - The individual should also give a definite indication of their consent – it is likely that mere acquiescence would not be sufficient.
- 9.2. The processing is necessary for the performance of or for entering into a contract with the individual concerned (i.e. an employment contract).
- 9.3. The processing is necessary for the Council to comply with a legal obligation. This will include performance of a statutory function and exercise of public law functions in the public interest.
- 9.4. The processing is necessary to protect the vital interests of the individual concerned.
- 9.5. The processing is necessary to pursue a legitimate interest of the Data Controller (i.e. the Council) or a third party to whom the data is disclosed.

In the majority of cases when data is obtained from individuals for processing it will be either advisable or necessary to obtain the individual's explicit consent.

If the data is 'Sensitive Data' then at least one of the following conditions must also be complied with:-

- 9.6 The individual has given their explicit consent to the data being used. This will be more onerous than the unambiguous consent needed for non-sensitive data.
- 9.7. There is no specific requirement for written consent but it is advisable that such consent is not merely given orally.
(One way to ensure that explicit informed consent is given for the processing of sensitive data would be to obtain the data from the individual by means of a form completed by each individual. Such a form could request specific data for specific purposes and would require the individual to indicate their consent by signing the form.)
- 9.8. If the data is being obtained directly from the individual to whom it relates it would be advisable if their explicit consent is obtained in every case. However if this is not possible or if the data is not being obtained from the individual concerned it can only be obtained if the processing is necessary.
- 9.9 To perform a legal obligation imposed on the local authority in connection with employment.
(This would apply for example to the personal details of the local authorities employees where such details were 'sensitive'.)
- 9.10 In order to protect the vital interests of the individual or another person and the consent of the individual cannot either be given or obtained or has been unreasonably withheld.
- 9.11 In connection with threatened or current legal proceedings.
- 9.12. To identify and ensure equality of treatment of individuals of different racial or ethnic origins. This will only apply to data concerning individuals race or ethnic origin.

(To come within these provisions the processing must be objectively justifiable and it is likely that the situations in which sensitive data can be obtained other than with the consent of the individual to whom it relates will be interpreted narrowly.)

10. What rights do individuals have under the DPA?

10.1. The right of access to information about themselves which we process

The individual or data subject has a right of access to information that we as a Council hold about them. They have the right to request in writing, and on payment of a fee (which is currently £10) to receive the following information:-

- 10.1.i Whether we process information about them.
(Any individual whose personal details are being processed by the Council have the right to be informed that the Council is processing data about them)
- 10.1.ii If we do, we must tell the individual the purposes for which we hold it and the recipients or classes of recipients to which the information may be disclosed. If the individuals conduct, reliability or creditworthiness is being assessed on the basis of the data they must be informed as to the logic/rationale behind this. The actual recipients of the data or class of recipients must be stated to the individual subject to certain qualifications
- 10.1.iii The information that we hold about the individual. We must provide a description of the personal details that we are processing.
- 10.1.iv The source of the information. If the data was not obtained from the individual the Council must identify to the individual the source of the data

This information about an individual must be supplied within a reasonable time, which must not, in any event, be more than 40 days from the date on which the request is received in writing, the fee is paid and the individual has adequately identified themselves.

All requests made by an individual to obtain the information listed above must be made in writing. The request should specify which description(s) of their personal data they wish to obtain. The Council have a specific 'Subject Access Request Form' for this. Copies of it are available from:-

Data Protection Officer
Social and Housing Services
c/o Civic Centre
Plymouth
PL1 2EW

The Council will only provide the information described above to an individual if the individual can provide enough information as the Council reasonably requires to satisfy itself of the individuals identity.

The Council will not provide all the information listed above if doing so would disclose information about another individual a 'Third Party') and that individual could be identified from that information, unless:

- the other individual gives their consent
- the Council considers it reasonable to provide the information without the other individuals consent.

The Council will however provide as much of the information as possible without identifying the other individual. Therefore all references to Third Parties must be deleted from the information that is provided to the Data Subject.

10.2. The right to serve a notice to us to cease processing data about them

Subject to certain conditions an individual is entitled to give written notice to the Council to cease processing or not to commence processing data concerning that individual if the outcome of processing the data is causing or likely to cause substantial and unwarranted damage or distress to the individual.

An individual may also request that the Council cease processing data about them after a reasonable period if the purpose of processing the data is to allow advertising or marketing material to be directed to the individual.

The Council must respond to such a Notice within 21 days of the receipt of the Notice, stating whether they have ceased or intend to cease processing the data or stating on what basis they consider the Notice to be unjustified.

If the Council continues to process data about an individual following service of a Notice, the individual may apply to the Courts for an order that the Council comply with the Notice. The individual will need to demonstrate to the satisfaction of the Court that the processing of the data will cause or is causing them substantial and unwarranted damage or distress.

11. What is Notification and Registration?

A register is held by the Information Commissioner of all organisations who hold personal information about individuals. Organisations who hold information about individuals like the Council are called 'Data Controllers'. The City Treasurer acting on behalf of the Council must send a Notification to the office of the Information Commissioner each year setting out the following:-

- The categories of data subject
- The type of information held
- The source from which it is obtained
- The purpose for which it is held
- The people or classes of people to whom it may be disclosed

A fee is payable by the Council each year. When the Council renews its Registration it must also update its entry if this is relevant.

12. What remedies are available to people if the DPA is breached?

There are 2 types of remedy available under the DPA for its breach.

- 12.1. An individual may take private action in law for damages if inaccurate or damaging information is held or if a Data Controller does not cease to process or use information in a damaging or unwarranted way when requested to do so.
- 12.2. Any failure by a Data Controller to properly register and notify its details to the Information Commissioner is a criminal offence and is liable to a fine. If the failure can be attributed to an individual within the organisation that individual may be liable for prosecution and the Data Controller may be prevented from processing that data.

13. Are there any exemptions to the DPA?

There are a number of detailed provisions of the DPA and in the Regulations which accompany the DPA which exempt or regulate particular types of information.

The following purposes are exempted from certain provisions of the DPA;

- National security
- Crime and taxation
- Health, education and social work
- Regulatory activities
- Journalism, literature and art
- Research, history and statistics
- Public inspection
- Corporate finance
- Examination marks
- Disclosures required by law
- Legal proceedings
- Domestic purposes
- Confidential references
- Armed forces
- Judicial appointments and honours
- Crown or Ministerial appointments
- Management forecasts
- Negotiations
- Examination Scripts
- Legal professional privilege
- Self-incrimination

Human Rights

What effect does the Human Rights Act 1998 ('HRA') have on DPA?

The HRA incorporates into English Law the provisions of the European Convention of Human Rights and Fundamental Freedoms (the 'ECHR'). There are 2 rights which have a bearing on the operation of the DPA:-

- The right to respect for private and family life (Article 8 ECHR), and;
- The right to freedom of expression (Article 10 ECHR)

Article 8

This article is the basis for the protection of privacy. The DPA is based upon a European Union Directive, which was drafted so as to enforce the protection of the rights contained within Article 8 of the ECHR. The DPA therefore complies with the European Union Directive and consequently with Article 8 of the ECHR.

Article 10

This article is the right to freedom of expression. This includes the right to receive and impart information without interference from a public authority (i.e. the Council). This is not an absolute right and is subject to a number of limitations. The principal limitation concerns the potential for conflict between the operation of Article 10 and Article 8. The right to freedom of expression and the right to personal privacy may conflict when personal information about an individual is processed and will be subject to the doctrine of proportionality.

The application of the HRA

Under Section 6(1) HRA the Council must act in a manner compatible with the rights contained within the ECHR. In practice, complying with the provisions of Article 8 should be achieved by complying with the DPA. Any potential conflict is more likely to arise between the terms of the DPA and Article 10.

In either case, it would be a defence to any action that the public authority had no choice but to act in the manner in which they did under the DPA. This coupled with the fact that the DPA is designed to protect the right contained within Article 8 of the ECHR, means that compliance with the terms of the DPA should enable a public authority to comply with the provisions of both the HRA and the ECHR.

Section 3(1) HRA provides that all primary and sub-ordinate legislation, such as Acts and Statutory Instruments of the UK Parliament promulgated under them must, 'be read and given effect in a way which is compatible with the Convention rights'. Therefore, when a Court, a Data Protection Tribunal or the Commissioner consider any of the provisions of the DPA they must ensure that they interpret specific provisions, if possible, so that they are consistent with the protection of rights contained within the HRA.

Freedom of Information

How does the Freedom of Information Act 2000 ('FOIA') link in with the DPA?

The FOIA became law on the 30th November 2000 and like the DPA is enforced by the Office of the Information Commissioner.

What does the FOIA cover?

The FOIA gives a general right of access to information of all sorts held by public authorities (i.e. the Council and those providing services for them) and sets out exemptions from that right and places a number of obligations on the Council.

When does the FOIA come into effect?

The FOIA must be brought fully into effect within 5 years of the 30th November 2000. With respect to the Council we had to forward to the Office of the Information Commissioner a Publication Scheme (please see below) by the 31st December 2002. The public will have a right of access to all the information listed within our Publication Scheme which is not described as being exempt information under FOIA from January 2005.

What rights do individuals have under FOIA?

Individuals have a right to their own information held on computer and in some paper files under DPA. As far as public bodies are concerned the FOIA will extend an individuals rights to allow access to all the types of information held, whether personal or non-personal.

An individual who makes a request for information must do so in writing, the FOIA itself gives applicants two related rights:-

- the right to be told whether the information exists
- the right to receive the information (and where possible, in the manner requested i.e. as a copy or summary, or the applicant may ask to inspect a record).

What is a Publication Scheme?

The FOIA places a duty on public authorities to adopt and maintain publication schemes, which must be approved by the Information Commissioners office. These publication schemes set out the type of information which the authority publishes, the form in which that information is published and give details of any charges. The Council's Publication Scheme has been approved by the Information Commissioners Office.

How do we respond to an individuals request under FOIA?

The Council will need to respond to a request for information under the FOIA within 20 working days (Please note that's less than the 40 days under DPA!). A fee may be charged, which must be calculated with reference to the FOIA's Fees Regulations. If a fee is required the 20 working days will be extended by up to 3 months until the fee is paid. In cases where information is covered by an exemption, the Council will then be required to consider the public interest in releasing it, this information must be provided within a reasonable time.

What types of information need not be released under FOIA?

There are 23 exemptions contained within the FOIA, some of which are similar to those under the

DPA (i.e. information need not be released if it would prejudice national security, or law enforcement).

Under the FOIA, some exemptions apply to a whole category (or class) of information, for example:-

- information relating to investigations and proceedings conducted by public authorities
- court records
- trade secrets

Information covered by these class-based exemptions is always exempt.

Other exemptions are subject to a prejudice test, for example, where the disclosure would, or would be likely to prejudice:-

- the interests of the United Kingdom abroad, or
- the prevention or detection of crime

Information only becomes exempt where disclosure would or would likely prejudice the activity or interest described in the exemption. In most cases where information is exempt the public authority must consider the public interest in providing the information. This public interest test involves considering the circumstances of each particular case and the exemption that covers the information. The information may only be withheld if the public interest in withholding it is greater than the public interest in releasing it.