



Data Protection Code of Practice

Final

May10 v1.4.doc

Table of Contents

Table of Contents.....	2
Document Control.....	3
1. Introduction.....	4
1.1 The UK Data Protection Act.....	4
2. Principles.....	5
2.1 Principle 1 – Fair and Lawful Processing.....	6
2.1.2 Conditions for Processing.....	7
2.1.3 Keeping Within the Law.....	7
2.1.4 Common Law Duty of Confidentiality.....	8
2.3 Adequate, Relevant, Not Excessive.....	8
2.4 Accurate and Kept up to Date.....	9
2.5 Not Held Longer than Necessary.....	10
2.6 Data Subject Rights.....	10
2.7 Security.....	12
2.8 Overseas Transfers.....	12
3. Notification.....	14
4. Exemptions.....	14
5. Disclosures.....	16
6. Complaints and Non-Compliance.....	18
Appendix A - Definitions.....	21
Appendix B - Sensitive Data.....	23

Document Control

Organisation	Torbay Council
Title	
Creator	Kelly Prince – Information Governance Advisor
Source	Data Protection Code of Practice
Approvals	
Distribution	
Filename	
Owner	Torbay Information Governance Team
Subject	Data Protection
Protective Marking	
Review date	

Document Amendment History

Revision No.	Originator of change	Date of change	Change Description
1.1	Information Governance manager	May 08	Amendments to Formatting and other information
1.2	Information Governance Advisor	Sep08	Amendments to formatting
1.3	Information Governance Advisor	Jun09	Review Document
1.4	Information Governance Advisor	May10	Final Review and Publication

Torbay Council

Data Protection Code of Practice

1. Introduction

The Council has a need to process accurate and relevant information about individuals in order to provide efficient and effective public services, often in partnerships with other organisations. In return the Council and all its' employees must accept their responsibilities for a demonstrable commitment to security of information, and respect for confidentiality. The Council wishes to be quite open about the type and extent of personal information that it holds.

This mandatory Code of Practice supports the Council's related Corporate Policies that are available on Torbay Council's Intranet. It applies to all employees within the Council; voluntary workers and elected members, or any other persons authorised to use any Council computer or information system (including paper files).

One of the ways in which the Council can ensure that any information about an individual is processed fairly and lawfully is to have regard to the UK Data Protection Act, 1998. The Act's main aim is to safeguard the rights of individuals, in particular their right to privacy. It applies to personal information that is processed by an organisation and collections of information where individuals can be identified and it includes eight Principles of legally enforceable good practice.

1.1 The UK Data Protection Act

The Data Protection Act, 1998 applies to information relating to living identifiable individuals whether it is processed automatically on computer, in electronic images (such as on closed circuit TV), or manually (such as on paper or in a card index system). This is known as personal information or data. It includes information that is archived, word-processed, used for testing and back-ups, and covers intentions and opinions in relation to the individual who is the subject of the personal information.

Personal data

Personal information or "personal data" can be as simple as a name and address, or just a postcode, if it means that a person can be identified from it, or from other information in the possession of the Council (or that is likely to come into our possession).

The individuals to whom the personal data relate are called "data subjects" and can be of any age. The Act **does not apply** to statistical or anonymous information where individuals cannot be identified; neither does it apply to people who are deceased

Processing

The Data Protection Principles apply to personal data that are 'processed'. Processing includes:

- obtaining
- holding
- amending
- collating and compiling
- reading and consulting
- disclosing
- transferring
- blocking, deleting or destroying information

To come within the scope of the Act, manual records must:

- **Identify the individual** - by name or other information such as a pay reference;
- **Be structured** either by reference to individuals or by reference to criteria relating to them **and** in such a way that **the information is readily accessible**. To determine whether information is "readily accessible" or not, the "temp test" should be applied. Ask yourself: "Would a temporary member of staff who is not familiar with the Council be able to access this manual filing system and retrieve personal data quickly and easily?" If the answer is yes, then the personal data are covered by the Data Protection Act.

2. Principles

'Processing' refers to anything done to the personal information by the people processing it including:

- the organisation.
- Adaptation.
- alteration retrieval.
- consultation or use.
- disclosure of the data by transmission.
- dissemination or otherwise making available.
- Alignment.
- Combination.
- Blocking.
- erasure or destruction of the information or data.

One of the main aspects of Data Protection is ensuring that this type of processing is done within the boundaries of the law. There are a set of eight Principles by which the data being processed must adhere to.

2.1 Principle 1 – Fair and Lawful Processing

“Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

- **At least one of the conditions in Schedule 2 is met; and**
- **In the case of sensitive personal data, at least one condition in Schedule 3 is also met.”**

In order to comply with the act, it is necessary to ensure that the individual is aware of how their data is going to be used once they have provided it. Torbay Council places what is known a ‘Fair Processing Notice’ on all forms and information that requires the submission of personal information. This way individuals are made aware from when we first collect data what may happen to it.

The Fair Processing Notice should be:

- Concise, in plain English and easy to understand.
- Legible and not too small, or hidden away within other text.
- Clearly explained and consistent, if provided verbally.
- As simple as “The information you provide will be used to..... for the purpose(s) of/so that we can....., and may be disclosed to/shared with” or similar wording as appropriate.
- Give the name of a contact should a person want to talk about the Fair Processing Notice, for example the Information Governance Team at Torbay Council, and supply contact details as well.

There are some circumstances when a Fair Processing Notice does not have to be provided. These apply if the personal data are necessary:

- To be processed in compliance with a legal obligation - The National Fraud initiative data matching exercise;
- For the prevention or detection of crime - Benefit fraud;
- For the apprehension or prosecution of offenders;
- To carry out regulatory activities (such as those carried out by Trading Standards or Environmental Health);
- Where they are made public by law;
- To protect their confidentiality for management forecasts/planning;
- As a record of the intentions of Torbay Council in relation to negotiations with the data subject;
- Where legal professional privilege applies;
- For national security – Threats of terrorism etc;

2.1.2 Conditions for Processing

Torbay Council must also consider a number of conditions that must be met when processing the data, unless a relevant exemption applies.

The main aspect to the conditions is the necessity for the processing. There are many ways in which it can be ensured that this is adhered to, e.g:

- Ensure that consent has been given by the data subject to the processing.

That the processing is necessary -

- For the performance of a contract to which are data subject is a party.
- For taking of steps at the request of the data subject with a view to entering into a contract.
- To comply with any legal obligation to which the data controller is subject, other than any obligation imposed by contract.
- Protect the vital interests of the data subject.
- Administration of justice and any other functions conferred to by enactments, the crown, ministers or functions of a public nature exercised in the public interest.

2.1.3 Keeping Within the Law

You should also ensure that you comply with any other legal requirement for the processing of personal data. We will ensure that personal data are processed lawfully and make every effort to ensure we do not contravene any criminal, civil or common laws.

Examples of laws that apply to personal data are:

- Common law duty of confidentiality (see Section 2.1.4 below)
- Libel and defamation of character
- Computer Misuse Act 1990 (governs unauthorised access to computers\hacking)
- Regulation of Investigatory Powers Act 2000 and Lawful Business Practice Regulations 2000 (govern covert surveillance and monitoring (for example use of internet and email). Torbay Council has its own policy Guidance on the RIPA which can be found on the Torbay Council website.
- Copyright, Designs and Patents Act 1988 (governs intellectual property, use of software without copyright owner's permission, etc).

If there is a contravention of these and any other legislation when processing personal data, there maybe a breach of the Data Protection Act.

2.1.4 Common Law Duty of Confidentiality

You should respect any duty of confidentiality that may exist when processing personal data, for example before responding to requests for information to be disclosed.

The duty of confidentiality is based in common law and is subject to interpretation by the Courts. It is flexible and can change over time. Generally, a duty of confidentiality exists where information is disclosed or revealed to you **in circumstances** and on the **understanding** that it will not be passed on to anyone else. The relationship between the data subject and the recipient is important. For example there is a strong duty of confidentiality between a doctor and patient, or someone providing a counselling or support service and an individual seeking help.

The duty of confidentiality can be overridden if:

- Consent has been given by the data subject or someone genuinely acting on their behalf.
- Failure to disclose personal data may put the data subject or other people at risk of harm, or if there is an overriding public interest to release the information (for example in the interests of community safety).
- The disclosure is required to be made by law or court order.

2.2 Lawful Purpose

“Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be processed in any matter incompatible with that purpose or those purposes”.

Information must only be used for the purpose for which it was originally collected. If it is necessary to use the information in a new way, the individual must first be contacted and the proposed additional use of the information fully explained.

If there is a new method of data collection it is essential that this is conveyed to the Information Governance Team who will add it to the Data Protection Notification this is explained further in the policy.

2.3 Adequate, Relevant, Not Excessive

“Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.”

You must hold only the **minimum amount** of personal data necessary to enable you to carry out your work.

You should ensure that:

- This information is adequate, relevant and not excessive. The Council should only request or hold as much information required for the purpose(s) that you require it.
- You do not ask for more detail than is necessary, for example date of birth, if an age range is sufficient.
- The Commissioner also suggests that it will not be acceptable to hold information on the basis that it might possibly be useful in the future without a view of how it will be used (see ICO legal guidance).
<http://www.ico.gov.uk>

2.4 Accurate and Kept up to Date

“Personal data shall be accurate and, where necessary, kept up to date”

A definition of ‘inaccuracy’ can be found under s.70 (2) of the Act;

‘For the purposes of the Act data are inaccurate if they are incorrect or misleading as to any matter of fact.’

An opinion, which does not purport to be a statement of fact, cannot be challenged on the grounds of inaccuracy. Any opinions or comments that are recorded should be clearly marked as such, and always be of a professional nature. This could involve simply writing a phrase next to the comment or opinion stating that it is simply a statement of opinion and is in no way the opinion of Torbay Council. Then initialling it to prove who has written it.

You should take reasonable steps to ensure that changes in personal data or circumstances are recorded as soon as possible after an event.

The Council recognises the importance of reliable information both in the provision of its services to the public, and in order to facilitate its own operational needs and allow for effective decision making at every level of the authority.

Data quality is seen as a crucial part of the management of information by the Council, and the availability of complete, accurate and timely data is acknowledged as a cornerstone for supporting service delivery and demonstrating accountability.

In order to ensure the Council achieves data quality it needs to evidence how data, including personal data is processed and maintains its integrity throughout its life-cycle. This will be achieved by having procedures and guidelines which detail:

- **Accuracy of data:** Is the data correct and is it valid?
- **Accessibility of data:** Can the data be readily and legally collected? Can the data be easily retrieved by authorised individuals?

- **Completeness of the data:** Is the relevant data collected and are any omissions documented.
- **Consistency of data:** Are clear and accurate data definitions implemented and adhered to? Do the data definitions define what level of detail is collected?
- **Validity of the data:** Is the data up-to-date

This will help the Council evidence its compliance with the Accurate and Up to Date principle of the Data Protection Act.

2.5 Not Held Longer than Necessary

“Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes”.

Personal data must not be held for longer than necessary. Retention of personal data should be based on business need and in accordance with any professional guidelines or legal requirements that apply. Care must be taken to ensure that data is securely destroyed when no longer required.

The Council’s Retention Schedule must be followed when assigning retention/ disposal dates to any information, not just that containing personal data. The Retention Schedule is available on the intranet under the Information Governance pages, within the relevant section.

Personal data that are held for research, statistics or historical purposes may be held indefinitely provided they are not processed to support measures or decisions about data subjects and the processing does not cause them substantial damage or distress.

2.6 Data Subject Rights

“Personal data shall be processed in accordance with the rights of the data subject under this Act”.

Everyone has the following rights under the Data Protection Act:

- To see a copy of information held about themselves (this is usually done by means of what is called ‘a subject access request’).
- To be given a description of the purpose(s) for which the information is held, its recipients and of source.
- To prevent processing likely to cause them damage or distress.
- To prevent processing for direct marketing purposes.

- To request that no decision that significantly affects them is carried out solely automatically, without the involvement of people and to be informed of the logic involved.
- To apply to the Court for rectification, blocking, erasure and destruction of personal data.
- To seek compensation through the courts.
- To request an assessment by the Information Commissioner's Office.

If a request for access to personal data, or a written notice to stop processing personal data for direct marketing or other purposes, or a query regarding automated decision making is received, it must be passed to the Information Governance Team as quickly as possible. Requests for access to personal data may be made by someone else acting on the individual's behalf. Subject Access forms and details on how to complete them are available on the intranet under the Information Governance pages, within the relevant section.

When an individual makes a request to see a copy of information held about them, the Council is entitled to ask them for:

- A separate request in writing (see form)
- Evidence to confirm identity (such as birth certificate, driving licence)
- Sufficient information to locate the information requested
- A fee of £10.00 (VAT exempt)

Individuals have the right to:

- Be told if the Council or someone else on their behalf is processing their personal information (this includes having it but not using it)
- Be given a description of the personal information; the reason for it being processed and to whom the personal information is or may be disclosed to.
- See a permanent copy of the information that is held, in an easy to understand format. (with any codes or short-hand notes explained etc)
- Be told the source of the personal information held about them (except in limited circumstances)

It is essential that prior to any disclosure of personal data, the appropriate procedures have been followed so that every aspect of the disclosure has been taken into account. This will prevent any unnecessary breaches of data security and/or unlawful or unauthorised disclosure.

If you have any doubt about a disclosure or need advice on how best to disclose data, contact the Information Governance Team for assistance.

2.7 Security

“Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data”.

You must take appropriate security measures to ensure that personal data and the equipment that stores it, are kept secure. This includes carrying out a risk assessment to determine the extent of security required, eg. level of physical access (*keys etc*) this includes what types of locks there are, where the keys are kept overnight, are there a spare set anywhere in case of emergency.

Other factors that should be considered are Computer/network access, disaster recovery plans, back ups and any mobile / home workers. The risk of a security breach should be measured against cost of implementation of the security measures, the type of data involved and the likelihood of harm to the individual the data is about.

You should also take reasonable steps to ensure the reliability of staff that has access to the personal data that you hold, and ensure service providers fulfil their security responsibilities by including Data Protection and security requirements in contracts with them. Torbay Council has standard contract terms which include all the areas that need to be covered in terms of Data Protection, for further guidance on this contact the Information Governance Team.

2.8 Overseas Transfers

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

If personal data are to be transferred outside the European Economic Area, you must ensure that at least one of the Schedule 4 conditions is met (see below).

The European Economic Area consists of:

EU Member States: Austria; Belgium; Denmark; Finland; France; Germany; Greece; Italy; Luxembourg; Netherlands; Spain; Sweden; Ireland
Plus: Iceland; Norway; Liechtenstein.

New EU Members: Bulgaria; Cyprus; Czech Republic; Estonia; Latvia; Lithuania; Hungary; Malta; Poland; Romania; Slovenia; Slovak Republic.

Please note that the above list may change as new countries are included in the European Economic Area.

The European Commission can decide if a country has an adequate level of protection for personal information. Currently, Argentina, Canada, Guernsey, Isle of Man and Switzerland are considered adequate.

Also information may be transferred under the United States' Department of Commerce's Safe Harbour Privacy Principles and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection.

Compliance with the other Data Protection Principles should still take place such as ensuring data is transferred securely by e-mail.

Schedule 4 Conditions for Transferring Personal Data outside the EEA

- The data subject has consented to the transfer.
- There is a contractual agreement in place requiring the recipient to comply with the Data Protection Principles.
- The country already has adequate Data Protection legislation or "safe harbour" agreements in place. A list should be available on the Information Commissioner's website at www.ico.gov.uk
- Performance of a contract between the data subject and Torbay Council (or for the taking of steps with a view to entering into a contract).
- Conclusion or performance of a contract between Torbay Council and a third party which is entered into at the request of the data subject or in their interests.
- Public register made available for inspection by law.
- Protecting the vital interests of the data subject or another person.
- Substantial public interest (as specified by order of the Secretary of State).
- In connection with any legal proceedings (including prospective ones, obtaining legal advice and for establishing, exercising or defending legal rights).
- If safeguards are in place, such as on terms authorised and approved by the Information Commissioner and provide adequate safeguards for the rights and freedoms of individuals.
- The transfer has been authorised by the Information Commissioner.

This requirement can apply to information that is published or made available on the Internet, or sent overseas by email.

The Council must also be appropriately notified for disclosures to other countries to take place. Contact the Information Governance Team to check this.

3. Notification

The notification register is a publicly available document, maintained by the Information Commissioner's Office, and is available on their website.

All systems that contain personal data (including manual records as well as computer systems) must be notified to the Information Governance Team, as well as any changes made to those systems that may affect our notification entry as the Council is required by law to keep its notification entry accurate and up to date.

The Council is required to notify:

- The purpose(s) for holding personal information.
- The kind of people who the information is held about.
- The types of information.
- Who it is disclosed to.
- Countries to whom it is sent to outside the European Economic Area.
- What kind of security and procedures are in place to protect the information (*this piece of information is not made public*).

It is essential that all Council staff keep up to date with the notification, and should ensure that they are acquainted with it at all times.

Each time that a change is required a form IT10 this can be found on the Intranet at <http://insight/it10-dp-notification.pdf> needs to be completed and returned to the Information Governance Team so that personal data can be processed lawfully by the Council.

4. Exemptions

"Data controller means:-

"A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed."

By law they can withhold certain kinds of exempt information - the main exemptions are set out below. Under the terms of The UK Data Protection Act, 1998 an individual does not need to be told whether exempt information has been withheld.

If an individual wishes to challenge the response they have received under an access to information request, they are within their rights to contact the Information Commissioner, who will investigate the situation.

It is important to remember that exemptions may not apply to the document as a whole, instead it may be necessary to apply them to small areas of the

document that cannot be disclosed. This involves what is known as redaction of the data, this is where it is simply deleted by some form or another.

The main exemptions are:

1. National Security (Section 28 of the Act)

2. Crime and Taxation

The prevention or detection of crime,
The apprehension or prosecution of offenders, or
The assessment or collection of any tax or duty or of any imposition of a similar nature

3. Health, Education and Social Work

This may relate to information that contains personal data regarding to social work or the mental or physical condition of the data subject

4. Regularity Activity

5. Special Purposes - defined as one or more of the following

The purposes of journalism

Artistic purposes

Literary purposes

6. Research, History and Statistics

7. Information made available to the public by or under enactment

8. Disclosures required by law

9. Disclosures made in connection with legal proceedings

10. Domestic Purposes

Miscellaneous Exemptions

1. Confidential references given by the data controller
2. Armed Forces
3. Judicial Appointments and Honours
4. Crown Employment and Crown or Ministerial appointments
5. Management forecasts/management planning
6. Negotiations
7. Corporate Finance
8. Examination scripts
9. Examinations marks
10. Legal professional privilege
11. Self incrimination
12. Transitional exemptions

5. Disclosures

Handling Disclosures

There must not be disclosure of any information unless authorisation has been given or it is known that it is permissible to do so. All Council employees must be aware of circumstances when information can be disclosed and to whom. There is general guidance on disclosures on the Information Governance webpages under the relevant section. For detailed advice contact the Information Governance Team.

In some cases, the Council has entered into an information sharing agreement, or protocol, with other organisations or Council departments. This type of agreement will cover circumstances such as the disclosure of data and any associated procedures which must be followed.

Generally when disclosing information always be aware of the following:

- If you receive a large amount of information, always check that you are only releasing the minimum amount that is actually needed.
- When passing information on that has come from third parties, like the Police, it is essential that you check that the information provider has given consent to the disclosure.

It is important to be aware that when information is disclosed to another Council department, it is made clear that this may result in the information being used for another purpose, when these occasions arise it is important to ensure that there is a suitable and up to date Fair Processing Notice.

Individual requests for Information

There are several ways an individual can request information about themselves which may necessitate careful consideration before release of the information:

1) Asking about the progress of an application they have made, or asking a question about their situation. Even though they are asking for details about themselves this is still regarded as a disclosure of information. Even though there are not usually any problems with disclosure of the information in these instances, it is still sensible to take precautions to ensure that the Council does not inadvertently disclose information about a relative or family member who lives at the same address.

2) There also maybe occasions where an attempt may be made to find out confidential information by someone who is actually impersonating the true individual. If a request is received that asks for information to be sent to another address apart from that held in the Council's

records, further proof is required to ensure that the person who is requesting the information is who they say.

The extent of the checks on the individual's identity should depend on the nature of the information being disclosed. In regards to third party then adequate evidence is also required in order to prove authorisation. The Council has standard forms for many disclosures to third parties (eg. the Police) which should be used to provide evidence that all necessary controls were applied to the disclosure.

If there are any doubts regarding the identity of the person requesting the information then the information should not be disclosed.

Disclosure of information by telephone

When requests for information are made over the phone the risk of unauthorised disclosure is higher, and there are a variety of safeguards that must be applied before disclosure is allowed:

- Ask the enquirer their name, address and some information that would be unique to the person only, such as an account number etc.
- Inform the enquirer that due to the nature of duty of confidentiality that a response can only be made in writing.
- Send the information in writing to the address that is known to you as the enquirer's.
- Ring back with the information to the telephone known to you as the enquirer's.

In cases where a member of staff is unsure whether or not to disclose the information, then the person should agree to call the requestor back and consult the line manager.

Requests in Person

Proof of identity is needed when a person requests information and wants to collect it in person. There are a variety of types of identification that are acceptable:

Driving licence	NHS Medical card	Allowance/pension book
Passport	Bus Pass	AA/RAC Card
Council Rent book	Official letter (solicitors)	Long term season ticket
Council issued SWIPE or smart card	Utility Bills	

Further authorisation can be gained by again asking questions that would be unique to the requestor for example a National Insurance number or a date that a payment is due (housing benefit etc).

Requests for information by correspondence

When a request for information comes in via letter or a third party's official form, the response can be sent back to the address that is retained by the Council providing that this is the address that is in the letter or in the request. When this is different the member of staff should take reasonable steps to ensure that they have taken reasonable care in checking out the identity of the requestor, as detailed above.

When can information be disclosed

Generally, information can be disclosed in the following circumstances:

- 1) When the individuals have been clearly informed about it.
- 2) With the consent of the individual or someone acting on their behalf.
- 3) To organisations or individuals acting on behalf of the Council.
- 4) If it required by law.
- 5) Crime Prevention or Taxation.
- 6) Vital Interests and Serious harm.
- 7) Research, Statistical and historical purposes.
- 8) In connection with Legal Proceedings.
- 9) Where information is made available to the public by law.
- 10) To safeguard National Security.

Further details on disclosure can be found on the Information Governance webpages under the relevant section. Remember that in all circumstances there may be control mechanisms which need to be applied (eg. using the standard Council forms), so check the Information Governance webpages for these resources.

6. Complaints and Non-Compliance

Data subjects are encouraged by the Information Commissioner's Office to make complaints regarding alleged non-compliance with the legislation directly to the organisation concerned in the first instance. If the complaint is not been resolved to the individual's satisfaction, s/he may then direct it to the Information Commissioner's Office. Data subjects may also seek compensation through the courts if they have been caused damage or distress. They may use the results of the Commissioner's assessment to support their case.

An individual who suffers damage or damage and distress as the result of contraventions of the requirements of the Data Protection Act are entitled to compensation. The Council must be able to prove that they have taken such care as deemed reasonable in all the circumstances to comply with the Act's requirements

Any complaints in relation to data handling/ processing and/ or disclosure received by Torbay Council must be directed to the Information Governance Team who will allocate an officer to undertake an internal review on behalf of the complainant.

Offences

Both employees and organisations may be liable for prosecution under the Act. If Torbay Council was found to be liable, legal action would be taken against the Chief Executive. If it is found that an employee is liable then s/he will face prosecution instead.

The main offences are:

- Obtaining and disclosing information without the consent of Torbay Council.
- Ignoring an Enforcement or Information Notice - An enforcement notice requires specific steps to be taken (or not) or to stop processing personal data, within a specified time period.
- Enforcing data subjects to make subject access requests (unless a statutory exemption applies).
- The procurement, sale, and offering for sale of personal data.
- Tampering with personal data which is subject to a subject access request.
- Deliberately providing false details to the Information Commissioner in notification or in an Information Notice or Special Information Notice.
- Failure to notify, not keeping a notification entry or registered address up to date.
- Obstructing a warrant.

Penalties

If found guilty of an offence, defendants can be sentenced to a fine of £5,000 if they go before a Magistrate's Court an unlimited fine can be imposed if the case is taken to Crown Court.

The offences of processing without notification, and enforced subject access are strict liability offences. This means that the Council may be criminally liable even if they did not intend to commit the offence and did not know that an offence was committed.

On conviction of an offender, the court may order any data connected with the crime to be forfeited, destroyed or erased.

Recently legislation has been passed which means that individuals can also be imprisoned for breach of the Act.

UK Regulatory Powers to fine

Organisations that deliberately or recklessly commit serious breaches of the UK Data Protection Act can now be fined by the Information Commissioner.

The Commissioner is empowered, following an amendment to the Data Protection Act 1998, to issue a 'monetary penalty notice' where there has been a breach of any of the Eight Data Protection Principles that is likely to lead to substantial damage or distress.

It is felt that this change within the law sends out a message to everyone that Data Protection must be a priority, and the prospect of large fines will act as a deterrent to ensure that organisations take their Data Protection obligations more seriously.

Appendix A - Definitions

Personal Information

Data which identifies a living individual, either directly from that information or from additional information which is in the possession of, or is likely to come into the possession of the data controller. It includes both factual information and expressions of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive Personal Information

Personal data consisting of information about racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sexual life, criminal proceedings or convictions.

Data Subject

The person the information is about.

Data User

Anyone processing personal information within the school. Data users have a legal duty to protect the information they handle. Information must be processed in line with the Data Protection Act 1998.

Data Controller

Person, company or organisation who determines the purpose and manner of the processing of the personal information (the school is the data controller).

Data Processor

These may be separate organisations that process information on behalf of data controllers (e.g. a third party company supplying confidential waste management services). Data processors also have obligations under the DPA and must ensure that the information they handle is processed in accordance with the legislation. A contract should always be put in place with any data processor to cover off DPA compliance.

Processing

Applies to *all* uses of data - collecting, storing, retrieving, reading, amending, and destroying.

Notification

The Information Commissioner maintains a public register of data controllers. Notification is the process of adding a data controller's details to the register. All data controllers processing personal information are required under the Data Protection Act 1998 to notify unless they are exempt.

The Information Commissioner

The Information Commissioner is an independent official appointed by the Crown to oversee the Data Protection Act 1998, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

Third Party

When this term is used in relation to personal data it means any person other than the data subject, the data controller or any data processor or other person authorised to process data on behalf of the data controller or data processor.

Consent

Consent is one of the grounds on which personal information may be processed lawfully. The data subject's consent is any freely given, specific and informed indication by which the data subject signifies agreement to personal information relating to him/her being processed.

Explicit Consent

In the case of sensitive personal information if consent is being sought it must be 'explicit'. The consent of the data subject should be absolutely clear and should cover the specific detail of the processing, the particular type of data to be processed (or even the specific information), the purposes of the processing and any special aspects of the processing which may affect the individual.

Appendix B - Sensitive Data

Sensitive data is defined as a 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 by them of any offence, or
- any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or court sentences.

There are exemptions where sensitive data may be processed without having to satisfy the conditions above. These are:-

- **Equal opportunities and fair treatment** - For the identification or review of the existence or absence of equality of opportunity or treatment between persons with a view to enabling such equality to be promoted or maintained. This applies to information about an individual's religious or other similar beliefs, or their physical or mental health or condition. The processing of this information must not cause nor be likely to cause substantial damage or distress to the individual or any other person. If the information is to be used to support measures or decisions to be made about an individual, their explicit consent must be obtained.
- **Confidential counselling, advice, support or any other services** - Where processing is necessary in the substantial public interest, and it is carried out without the explicit consent of the individual.
- **Prevention or detection of crime** – must be in the substantial public interest, where seeking explicit consent of the individual would prejudice these purposes.
- **Discharge of any function designed to protect members of the public against dishonesty, malpractice or other seriously improper conduct, unfitness or incompetence** – must be in the substantial public interest.
- **Disclosure of information for journalistic, artistic or literary purposes**, with a view to publication can take place where Torbay Council believes that publication would be in the public interest.
- **Insurance or occupational pension schemes** where details of relatives of the insured person or member are required, (for example

health details of relatives used to calculate the life expectancy of the insured).

- **Political opinions by registered political parties**, provided such processing does not cause substantial damage or distress to any person.
- **Historical, statistical or research purposes**, for example, in the course of maintaining archives. The sensitive information must not be used to make a decision about an individual without their consent, nor cause them any substantial damage or distress.
- **Processing carried out by the Police** in the exercise of their common law powers.