HOMELANDS PRIMARY SCHOOL

DATA PROTECTION POLICY

ADOPTED BY THE FULL GOVERNORS ON……28.06.06……

REVIEWED……27.04.10……

REVIEWED……30.04.13……

REVIEWED……19.01.16……

Rationale

Homelands School is committed to a policy of protecting the rights and privacy of individuals, including pupils, staff and others, in accordance with the DPA.

Homelands School needs to process certain information about its staff, pupils and other individuals with whom it has a relationship for various purposes such as, but not limited to:

- the recruitment and payment of staff
- the administration of programmes of study
- the recording of a student's progress

To comply with various legal obligations, including the obligations imposed on it by the Data Protection Act, 1998, Homelands School must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

Compliance

This policy applies to all staff and pupils of Homelands School. Any breach of this policy, or of the Act itself will be considered an offence and the school's disciplinary procedures will be invoked.

As a matter of best practice, other agencies and individuals working with Homelands School, and who have access to personal information, will be expected to read and comply with this policy. It is expected that departments who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which among other things will include an agreement to abide by this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the DPA and other relevant legislation.

The Code of Practice on Data Protection for Schools gives further detailed guidance and Homelands School undertakes to adopt and comply with the CoP.

The Data Protection Act, 1998

This piece of legislation came into force on the 1st March 2000. The DPA regulates the processing of personal data, and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/ manual files; electronic records; photographs; CCTV images), and may include facts or opinions about a person.

The DPA also sets out specific rights for school students in relation to educational records held within the state education system. These rights are set out in separate

education regulations 'The Education (Pupil Information) (England) Regulations 2000.' For more detailed information on these Regulations see the Data Protection Code of Practice for Schools (CoP).

Responsibilities under the DPA
Homelands School will be the 'data controller' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data.

The Head of the school is responsible for all day-to-day data protection matters, and s/he will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the school.

The Head is also responsible for ensuring that the school's notification is kept accurate. Details of the school's notification can be found on the Office of the Information Commissioner's website (www.informationcommissioner.gov.uk).

Compliance with the legislation is the personal responsibility of all members of the school who process personal information.

Individuals who provide personal data to the school are responsible for ensuring that the information is accurate and up-to-date.

Torbay Council's Information Governance Team will be available to provide advice and assistance to the Head.

Data Protection Principles
The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles. More detailed guidance on how to comply with these Principles can be found in the CoP. In order to comply with its obligations, Homelands School undertakes to:

1 – Process personal data fairly and lawfully
Homelands School will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller; the purposes of the processing; any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

2 – Process the data for the specific and lawful purpose for which it collected that data, and not further process the data in a manner incompatible with this purpose
Homelands School will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

3 – Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed
Homelands School will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will

always be drafted with this in mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

4 – Keep personal data accurate and, where necessary, uptodate
Homelands School will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the school if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the school to ensure that any notification regarding the change is noted and acted on.

5 – Only keep personal data for as long as is necessary
Homelands School undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means Homelands School will undertake a regular review of the information held and implement a weeding process when, eg. pupils or a member of staff leaves the school.

Homelands School will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (eg. secure electronic deletion; shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

6 – Process personal data in accordance with the rights of the data subject under the legislation
Individuals have various rights under the legislation including:

- a right to be told the nature of the information the school holds and any parties to whom this may be disclosed
- a right to prevent processing likely to cause damage or distress
- a right to prevent processing for purposes of direct marketing
- a right to be informed about the mechanics of any automated decision taking process that will significantly affect them
- a right not to have significant decisions that will affect them taken solely by automated process
- a right to sue for compensation if they suffer damage by any contravention of the legislation
- a right to take action to rectify, block, erase, or destroy inaccurate data
- a right to request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened

Homelands School will only process personal data in accordance with individuals' rights.

7 – Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data
All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

Homelands School will ensure that all personal data is accessible only to those who have a valid reason for using it.

Homelands School will have in place appropriate security measures eg.

- ensuring that hard copy personal data is kept in lockable filing cabinets/ cupboards with
  controlled access (with the keys then held securely in a key cabinet with controlled access)
- keeping all personal data in a lockable room with key-controlled access
- password protecting personal data held electronically
- archiving personal data on disks which are then kept securely (lockable cabinet)
- ensuring back up data kept off site to enable business continuity
- placing any PCs or terminals, CCTV camera screens etc that show personal data so that they are not be visible except to authorised staff
- ensuring that PC screens are not left unattended without a password protected screen-saver being used.

In addition, Homelands School will put in place appropriate measures for the deletion of personal data – manual records will be shredded or disposed of as 'confidential waste', and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal, or, if that is not possible, destroyed physically. A log will be kept of the records destroyed.

This policy also applies to staff and pupils who process personal data 'off-site', eg. when working at home, and in such circumstances additional care must be taken regarding the security of the data.

8 – Ensure that no personal data is transferred to a country or a territory outside the European Economic Area unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data
Homelands School will not transfer data to such territories without the explicit consent of the individual.

This also applies to publishing information on the Internet – because transfer of data can include placing data on a website that can be accessed from outside the EEA – soHomelands School will always seek the consent of individuals before placing any personal data (including photographs) on its website.

If the school collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

Consent as a basis for processing
Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner.

Consent is especially important when schools are processing any sensitive data, as defined by the legislation.

Homelands School understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (eg. via signing a form), whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

Homelands School will ensure that any forms used to gather data on an individual will contain a statement (fair collection statement) explaining the use of that data, how the data may be disclosed, and also indicate whether or not the individual needs to consent to the processing.

Homelands School will ensure that if the individual does not give his/ her consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

Subject Access Rights (SARs)
Individuals have a right to access any personal data relating to them which are held by the school. Any individual wishing to exercise this right should apply in writing to the Head of the school.
Any member of staff receiving a SAR should forward this to the Head of the school.

The school reserves the right to charge a fee for data subject access requests (currently £10).

Under the terms of the legislation, any such requests must be complied with within 40 days.

For detailed guidance on responding to SARs, see the CoP.

Disclosure of Data
Only disclosures which have been notified under the school's DP notification must be made and therefore staff and pupils should exercise caution when asked to disclose personal data held on another individual or third party.

Homelands School undertakes not to disclose personal data to unauthorised third parties, including family members, friends, government bodies, and in some circumstances, the police.

Legitimate disclosures may occur in the following instances:
- the individual has given their consent to the disclosure
- the disclosure has been notified to the OIC and is in the legitimate interests of the school
- the school is legally obliged to disclose the information
- the disclosure is required for the performance of a contract

There are other instances when the legislation permits disclosure without the consent of the individual. For detailed guidance on disclosures see the CoP.

In no circumstances will Homelands School sell any of its databases to a third party.

Publication of school information
Homelands School publishes various items which will include some personal data, eg.

- internal telephone directory
- event information
- staff information
- lists of pupils

It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential, or restricted to internal school access only. Therefore it is Homelands School's policy to offer an opportunity to opt-out of the publication of such when collecting the information.

Staff records appertaining to individual staff will remain of a confidential nature between the Head and the member of staff.

Email
It is the policy of Homelands School to ensure that senders and recipients of email are made aware that under the DPA, and Freedom of Information legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on the school's email.

Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from the school may be accessed by someone other than the recipient for system management and security purposes.

CCTV
There are some CCTV systems operating within Homelands School for the purpose of protecting school members and property. Homelands School will only process any personal data obtained by the CCTV system in a manner which ensures compliance with the legislation.

See further guidance on data protection available in school.

Data Protection Code of Practice

Contents:

Introduction

This Code of Practice on Data Protection has been prepared to give guidance to all schools processing personal data. It expands on information given in each school's Data Protection Policy, and should be used to facilitate the school's compliance with the legislation.

All schools need to collect and use personal information about students, staff and other individuals who come into contact with the school. In addition schools may be required by law to collect and use certain types of information to comply with statutory obligations of Local Education Authorities (LEA's), government agencies and other bodies. This personal information (whatever form it is in) must be processed within the terms of the relevant legislation.

The Data Protection Act 1998 (DPA) came into force on 1st March 2000. The DPA is based on eight legally enforceable principles which set out the conditions for processing personal information. All schools have a legal obligation to comply with the provisions of the DPA.

Notification

Processing personal information without a valid registration entry (notification) is a criminal offence. The school is responsible for notifying its processing of personal data with the Information Commissioner. The information is included in a public register of Data Controllers and can be found at www.informationcommissioner.gov.uk. The Head Teacher is responsible for ensuring the school's entry is kept up to date.

The Data Protection Act Principles

To comply with the DPA, all personal information must be processed in accordance with the eight Data Protection Principles.

Principle 1 - Processed fairly and lawfully

Lawful Processing: All processing of personal information must be lawful**. BEFORE** obtaining and using any personal information make sure that there is a lawful basis for processing, eg. in order to fulfil a statutory duty.

All processing must comply with one of the Act's conditions for processing:

1. The individual has consented to the processing
2. Processing is necessary for the performance of a contract with the individual
3. Processing is required under a legal obligation (other than one imposed by contract)
4. Processing is necessary to protect the vital interests of the individual (the Information Commissioner considers that reliance on this condition may only be claimed where the processing is necessary for matters of life and death ie disclosing medical history to a hospital department treating the data subject after a serious road accident)
5. Processing is necessary to carry out public functions eg. administration of justice
6. Processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could unjustifiably prejudice the interests of the individual)

The DPA makes additional provisions for the processing of '*sensitive'* personal information. Sensitive personal information includes 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

In order for sensitive personal information to be considered fairly processed, in addition to one or more of the standard conditions for processing personal information being met, *at least one of the extra conditions detailed below must also be met*:

1. Having the explicit consent of the individual
2. A requirement by law to process the information for employment purposes (eg. ethnic monitoring)
3. A requirement to process the information by law
4. Processing the information is required in order to protect the vital interests of the individual or another person
5. Dealing with the administration of justice
6. Where the information is required in connection with legal proceedings, obtaining legal advice or establishing legal rights
7. Processing is necessary for medical purposes (to be undertaken by a health professional)
8. It is required to carry out statutory functions of the school
9. The individual has made the information public themselves
10. Information about racial or ethnic origin is only collected to monitor equality of opportunity or treatment

The requirement to process information lawfully includes common law, such as the common law duty of confidentiality – where information has been given in confidence on the understanding that it will not be disclosed further without consent being obtained. If information is obtained "in confidence" always explain fully what this means at the point of collection.

Fair processing: In order to process information fairly, whenever information about individuals is first obtained or received, those individuals should be made aware of the following information:

- The identity of the organisation (or individual) they are giving their information to
- Why it is needed and what it may be used for (unless it is obvious from the circumstances)
- Whether it will be used for any other purposes, such as fraud prevention
- Any other individual or organisation it may be disclosed to (including those outside the school). Be as specific as possible and name organisations or individuals to whom information may be disclosed. It should also be made clear if information may be shared within the school as a whole, or with other specific departments
- How to obtain a copy of the personal information being held

In some limited cases, the above information does not have to be supplied, eg. if it is collected to carry out regulatory activities, or is required to be processed by law.

Principle 2 - Used only for the purpose it was originally obtained for

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.

Principle 3 - Relevant, not excessive, adequate enough to meet operational needs or legal requirements

Only collect sufficient information to enable the processing for which it was originally obtained. Information should not be held "just in case" it could be useful one day. Do not ask for more detail than is necessary (eg. asking for date of birth, when "over 65" will suffice).

Any opinions or remarks that are recorded about a person should be clearly marked as such; should always be of a professional nature, and should be able to be substantiated. Remember that individuals have the right to see a copy of all information that is held about them - including emails - subject to limited exceptions.

Principle 4 - Accurate and up to date

Information is defined as inaccurate if it is incorrect or misleading as to any matter of fact.

Information received from third parties

Where information about an individual is provided by someone else, it is important to make a note on the file of the following:

- Who gave the information
- Date it was received
- Who or what the information relates to
- A clear indication if the information is fact or opinion

This information is important to have if an individual makes a subject access request.

Always take reasonable steps to ensure the accuracy of the information received from third parties.

The individual should be informed that the school is holding information about them when it has been received this way, *unless* doing so would involve a "disproportionate effort" or would be likely to prejudice the prevention or detection of crime. Individuals should also be informed as to how the information will be used and disclosed, to satisfy the fair processing requirements.

If an individual has informed the school that, in their view, the information is inaccurate, then a note should be made next to the information that they have expressed this view, unless it is deleted or amended in accordance with the individual's views.

Always keep a record of when any information was last updated and last reviewed.

Handling information supplied verbally

Information received verbally should be double checked with the individual by repeating what they have said, especially if it is unclear what information is being given. Do not add any unnecessary comments when making a note, as they may be disclosable under a subject access request.

Principle 5 - Not kept for longer than is necessary

Remember that the Data Protection Act also applies to archived information, test data and backups, therefore information must be kept only for the length of time needed in order to fulfil the purpose for which it was obtained, eg. any time specified by statute; for legal purposes; or for valid business purposes.

The Records Management Society of Great Britain has produced a model records retention schedule especially for schools which can be found at www.rms-gb.org.uk. The need to keep all information should be reviewed regularly.

Principle 6 - Processed in accordance with the individuals rights

The DPA provides data subjects with a number of rights in relation to the information held about them. Everyone has the right:

- To see a copy of information held about them (make a subject access request)
- To prevent processing likely to cause damage or distress
- To prevent processing for direct marketing purposes
- To be informed about the mechanics of any automated decision taking process that will significantly affect them, and not to have significant decisions that will affect them taken solely by an automated process
- To apply to the Court for rectification, blocking, erasure and destruction of personal information
- To compensation
- To request an assessment by the Information Commissioner's Office

Principle 7 - Kept secure. Appropriate technical and organisational steps should be taken to safeguard personal information

This includes carrying out a risk assessment to determine the extent of the security required, including, physical access (keys etc); computer/network access; disaster recovery plans; backups, and mobile/home workers. Information must be protected from unauthorised or unlawful processing, and against accidental loss, destruction or damage.

Access to information

All information should have one or more nominated owners responsible for deciding who should have access. Levels of access should be appropriate for the specific requirements of an employee's duties and responsibilities, and must be regularly reviewed.

Access by external organisations or individuals

Access to personal information may be given to individuals or organisations acting on behalf of the school, providing a service to it or working in partnership with it. However, this access must be strictly controlled, given on a need to-know basis only, and reviewed regularly.

A contractual arrangement or information sharing agreement must be in place to govern access to information and systems. See Section 5 below on disclosures for further guidance.

Principle 8 - Not transferred abroad without suitable safeguards for the protection of the individual

Transfers to a country outside the European Economic Area may not take place unless the country can ensure an adequate level of protection for the rights and freedoms of individuals in relation to the processing of personal information.

The European Economic Area (EEA) consists of the 25 EU Member States (as of May 2004), together with Iceland, Norway and Liechtenstein.

The Act provides for specific circumstances where information may be disclosed overseas:

- With the consent of the individual
- If the transfer is necessary for the conclusion of a contract between the school and a person other than the individual, or for the performance of a contract
- If the transfer is necessary for reasons of substantial public interest
- Where the transfer is necessary for, or in connection with legal proceedings, for the purpose of obtaining legal advice, or for establishing, exercising or defending legal rights
- If the transfer is necessary to protect the vital interests of the individual
- Where the transfer is part of information provided on a public register
- Where the transfer is made on terms approved or authorised by the Commissioner as ensuring adequate safeguards for the rights and freedoms of individuals

This requirement needs to be complied with when information is published or made available on the Internet, or is sent by email to countries outside the EEA.

If personal information is published on the Internet, it may potentially be disclosed to anyone living in countries outside the EEA. Consent must therefore be obtained before any personal information is published/disclosed/made available on the Internet, and the school must also ensure that it is appropriately registered for worldwide disclosures to take place.

Fair Obtaining

Whenever information is obtained from, or received about, individuals, the individuals must know, be told, or have ready access to the following information (or if it is not possible at the point of collecting the information, they must be told as soon as practicable afterwards), regardless of the method of communication used:

- Who they are giving their information to
- Why it is needed and what it may be used for (unless it is obvious from the circumstances)
- Whether it will be used for any other purposes, such as fraud prevention
- Who it may be disclosed to (see below for further details)
- How to obtain the information held about themselves

The above information will not have to be supplied if it is necessary to process it solely:

- For national security

- For the prevention or detection of crime
- For the apprehension or prosecution of offenders
- To carry out regulatory activities
- As required by law

Or where:

- Information is made public by law eg. on the electoral role
- Negotiations might be prejudiced
- Legal professional privilege applies

Individuals must be told if information is intended to be disclosed outside the school to service providers or external organisations. Schools should be as specific as possible and name organisations or individuals to whom information may be disclosed. Where the list is very long, or there may be different third party service providers in future, then a generic description may be used, such as "healthcare providers" or "other local schools".

If information is required to be disclosed by law, the individuals do not have to be informed of this, but it is good practice to ensure that they are made aware of the statutory requirement to release information about them.

If information is obtained "in confidence" the meaning of this should be explained, if appropriate. It should also be made clear if information may be shared within the school as a whole or with other specific departments.

A 'fair obtaining statement' can be used as a way of informing individuals of how their personal information will be used when obtaining it. Fair obtaining statements can be used when collecting personal information (eg. on forms on websites). An example of a fair obtaining statement is outlined below (this can be amended to meet the requirements of different situations):

"Information held by [X] school complies with and is stored in accordance with the Data Protection Act 1998. The information you have provided here will be used to ***[do what ? insert here]*** *and may be disclosed to* ***[who ? insert here]*** *for the purpose of* ***[what is going to be done with the information – insert here]. [It may also be appropriate to add something here about any other disclosure which might be made and why]****"*

Disclosures

Disclosing personal information to other people, organisations or departments can only be made in certain circumstances. Some of the more usual circumstances for disclosure are listed below. For more detailed guidance, or any queries about disclosures in other instances, contact the Head Teacher in the first instance.

Generally, information should not be disclosed unless the school has the responsibility or authority to do so, and any information about individuals should be provided in an 'anonymised' form, if this is acceptable to the requester. There may be a breach of the Human Rights Act if personal information is disclosed when anonymised information would be sufficient.

When disclosing information:

- if a request for large amounts of information is received, always check to ensure that only the minimum amount that is actually needed to satisfy the request is released
- check that the information provider consents to any disclosure when passing information on that has come from third parties (eg. the police)
- care must be taken if disclosing to other departments as this may result in information being used for another purpose, different to the one(s) for which the information was originally obtained and would place the school in breach of the Data Protection Act.
- remember that some legislation imposes restrictions on disclosures of certain types of information. An example of this is the restriction on disclosure of HIV/Aids related information outside of Health organisations

Disclosures required by Law

Where information is required to be disclosed by law, there is no breach of the DPA principles regarding fair obtaining or processing, and individuals have no grounds for complaint that information was unfairly obtained, used or disclosed.

Examples of a legal requirement to disclose include:

- Health and Safety at Work Act 1974, Regulations on the Reporting of Injuries, Diseases and Dangerous Occurrences (1985 Sl No 2023 and 1989 No 1457)
- The National Fraud Initiative, which has become an annual large-scale data matching legal obligation. Affected individuals must be advised that it will take place.

If someone requests information quoting a requirement to disclose by law, ask for the specific statutory requirement to disclose to be given in writing, on their headed paper, including the Act, section and the specific wording relied on.

When making a disclosure record what information was disclosed, the statutory basis for releasing it, who it was given to and when.

Note: some laws only give statutory power to make a disclosure or share information, not a legal duty. An example of this is the Crime and Disorder Act 1998, Section 115. Disclosures must still comply with the Data Protection Act and other laws. Requests for information under the Crime and Disorder Act may be governed by Information Sharing Protocols.

Disclosures of information under Section 29 of the DPA

The Data Protection Act allows disclosures to take place for the prevention and detection of crime, or the apprehension or prosecution of offenders, but only for criminal law. Anyone making such requests must have the legal powers, such as the ability to bring prosecutions or take legal action. If in any doubt, consult Torbay Council's Information Governance Team.

There must always be a substantial risk, rather than a mere chance, that failure to have the information would noticeably damage crime prevention/apprehension/prosecution purposes.

Such requests must be made on an individual case by case basis. *"Fishing expeditions" are not permitted.* Information about more than one individual may be requested, provided there is sufficient justification.

All disclosures must be recorded and filed with the Section 29(1) form (see appendix 4), in case of subsequent legal claim or complaint from the individuals concerned. Similarly, any requests that are declined must also be documented, with reasons for not providing the information.

Section 29 is limited to criminal proceedings and does not cover civil proceedings.

It is the responsibility of the person or organisation who discloses information to make sure they have reasonable grounds for disclosing the information. It should be noted that there is no legal requirement to disclose information for crime prevention purposes.

Vital interests and serious harm

Disclosures may be made without breach of the Data Protection Act:

- to protect the vital interests of the individual, for example a release of medical information where failure to release it would result in harm to, or the death of, the individual
- to prevent serious harm to a third party that would occur if the information was not disclosed

Always keep a record of what information was disclosed, to whom, when and for what reason.

In connection with legal proceedings

Information may be disclosed, where it is necessary:

- for the purpose of, or in connection with any legal proceedings (including future prospective legal proceedings)
- for the purpose of obtaining legal advice
- for the purposes of establishing, exercising or defending legal rights

It can be difficult to determine whether the information is 'necessary' for legal proceedings, obtaining legal advice or defending legal rights. Unless it is obvious that the provision of this information is necessary, it is advisable to refuse the request. The requester can always apply to the court to obtain a court order to obtain the information. *A court order requires disclosure of the information.*

All disclosures (or decisions to withhold information) must be recorded.

Buying in services

Sometimes it is necessary to employ third parties to provide services for schools. All such contractors that have access to personal information should know how to take care of it and be able to guarantee compliance with Data Protection Principles.

Contractual terms should be drafted, to detail:

- who owns the information – if it was collected for the school, it remains the school's information not the contractors
- a confidentiality clause
- compliance with the principles of the DPA – as specific and clear as possible. Include details on access, security controls, and how breaches will be dealt with
- who deals with subject access requests
- what happens if work is sub-contracted
- an indemnity clause

It is the responsibility of the school, as data controller, to take reasonable steps to ensure that contractors comply with all Data Protection Principles, and that any alleged breaches are investigated.

Partnerships and information sharing

Some external parties working in partnership with schools may request access to information or systems. Before sharing information with a partner:

- make sure the school has the legal powers to share information in the first place - if this does not exist, generally the information cannot be shared - even with consent of the individuals. If there is any doubt, check with the Torbay Council Information Governance Team
- ensure individuals know that the information may be used in this way. Their consent to disclose will be required, unless the school is required by law to share the information for this purpose. If there is a legal requirement, make sure that the piece of legislation and section within it which requires access or sharing of the information is documented
- ensure that there is a written information sharing agreement, protocol or contract in place that specifically includes data protection compliance, with instructions on use and disclosure of information intended to be shared
- access must be on a strict need to know basis and must be appropriately controlled. Any partners must not have access to more information than needed, including any access to staff email/address information, Intranet, and network drives.

Disclosing information about the person requesting it

Often an individual will contact the school to ask a question about their own situation, eg. a member of staff enquiring about the number of days they have been off sick; or a parent asking what data the school holds about them in connection with some voluntary work they have undertaken at the school. This will still be a disclosure of information. Usually there is no problem releasing it but precautions have to be taken to avoid unauthorised disclosures, eg. providing information about or to someone other than the applicant, for example, a relative living at the same address.

The extent of the precautions required and checks as to the individual's identity will depend on the nature of the information being disclosed. Particular care should be taken if an individual requests information by telephone. In such instances it is recommended that the individual is informed that for reasons of confidentiality, a reply can only be given in response to a written request.

When disclosing information the following are acceptable as proof of identity:

• Passport	• Driving Licence	• Birth Certificate
• Recent utility bill	• Official Letter (Solicitor, etc)	• Bus Pass

Wherever possible, it is advisable to back up identity checks by asking further information known only to the enquirer and the school.

Information must never be given to third parties without adequate evidence to prove authorisation.

Requesting Information Required By Law

There may be times when a school needs to request information which it is required to process by law. Where this is the case, make the request in writing (on headed paper) clearly stating the relevant piece of legislation which requires the information to be provided.

Marketing

Where personal information is going to be used for secondary or non-obvious purposes, particularly where it may be used or passed on for direct marketing purposes, give the individual the opportunity to opt-in, or to give their consent for this purpose. Where the individual has not opted-in it cannot be assumed that they have given their consent for processing. Note: some PTA functions may be considered to be direct marketing.

The Telecommunications Regulations require that individuals must consent to their information being used for direct marketing purposes by telephone, fax or email. For more information, see the Direct Marketing Association Website at www.the-dma.org.

Remember that individuals have the right under the Data Protection Act to prevent their personal information from being processed for direct marketing purposes.

Photographs and Internet Publishing

Photographs are classed as personal data, therefore the use of photographs is covered by the DPA. If the school intends to publish photographs of pupils and staff on the school website or other printed publications for promotional purposes, it must be processed fairly and lawfully.

It must always be made clear that the school could use the photographs on the school website, as well as in printed publications for promotional purposes. It is also important to make it clear that websites can be viewed world wide by anyone with access to the internet.

If photographs of children are to be used, then generally children over the age of 12 are deemed able to give their own consent. Children under this age should have the countersignature of their parent/guardian (ideally the child should also give their consent). It may be that the best solution in most circumstances is to gain consent from both parents and child, regardless of age.

Note: consent can be withdrawn at any time, so the photograph must be able to be removed if consent is withdrawn.

Before using photographs already held on file, it is recommended that the consent of all individuals in the photograph is renewed. Photographs of pupils who have left the school should not be used and should be destroyed. If photographs are received from an agency, it is ultimately the school's responsibility to make sure the agency has gained consent – always get this in writing. See appendices 5 and 6 for consent forms.

The length of time consent is valid for is an important consideration when using images of children as they change quite quickly. It should also be considered that the child in the image may not want an old picture of themselves to be seen. It is therefore suggested that the photograph is held (together with the consent forms) for 2 years from the date the consent form is signed. If it is held for a longer period, the image will definitely be out of date and inaccurate.

The National Grid for Learning has further information and guidelines on using photographs on the internet for schools at http://safety.ngfl.gov.uk/schools/

Copyright

It is important to consider the copyright position of any photographs being used, as they are covered by the laws of copyright. The right covers copying, adapting, issuing copies to the public, performing in public and broadcasting the material. Copyright is automatic and does not depend on the completion of any formalities, such as registration. More information on copyright is available from the Copyright Licensing Agency at www.cla.co.uk

CCTV

The type of camera and the actual way in which the CCTV system is used will determine whether or not it is covered by the DPA, and if CCTV needs to be included as one of the purposes in the school's notification entry.

For the images to be classed as personal information (ie. relating to the individual and affecting their privacy), the following points must be considered:

- The person has to be the focus of the information
- The information indicates something significant about the person

If a static camera is used for general security purposes; it does not focus on individuals; the zoom facility is not used/ it does not have a zoom facility, then it will not be covered by the DPA.

If the camera can be remotely operated, can zoom in (it has pan and zoom facility), or track an individual, then it will be covered by the DPA.

Adequate signage must be in place to inform people when any CCTV system is in operation, and its purpose. It must also include details of the data controller and contact details.

Note: failure to comply with the DPA may also affect the police's ability to use the CCTV images to investigate a crime, and may therefore hamper the prosecution of offenders.

If the images caught on camera constitute personal data, then they may need to be disclosed in the event of a subject access request.

If an external company is providing, maintaining and controlling the CCTV system, they should have a current Data Privacy Statement, and procedures for processing subject access requests, with which the school should be familiar. Please See PPP CCTV Data Protection Plan attached to this Policy

CCTV tapes should be stored in a secure locker with access restricted to the Head Teacher. Tapes should be kept for a period of 28 days before being re-used. Each time the tape is used, the date should

be written on the tape. A separate log should also be kept detailing when the tape was changed and the person responsible.

A log should also be kept detailing any tapes that have been viewed by Council staff or police (or anyone else), the reason for viewing, and any relevant log numbers. If the police remove the tape, or a copy of it, this should also be recorded on the log, and the police should undertake to confirm destruction (or return) of the tape as appropriate.

Anyone applying for School CCTV images under a subject access request should complete the standard subject access form. If the police request the data, a Section 29 form (see appendix 4) must be completed. If a subject access request for CCTV recordings is received, please contact Torbay Council's Information Governance Team.

For further guidance on CCTV, including the use of digital recording CCTV systems, please contact Torbay Council's Corporate Security Officer. Further information on best practice for CCTV use can be found in the National User Group CCTV code of practice.

Individual rights

Rights of Data Subjects

The DPA provides data subjects with a number of rights in relation to the information held about themselves. Everyone has the right:

- To see a copy of information held about them (make a subject access request)
- To prevent processing likely to cause damage or distress
- To prevent processing for direct marketing purposes
- To be informed about the mechanics of any automated decision taking process that will significantly affect them, and not to have significant decisions that will affect them taken solely by an automated process
- To apply to the Court for rectification, blocking, erasure and destruction of personal information
- To compensation
- To request an assessment by the Information Commissioner's Office

Routine enquiry or data protection subject access request?

Schools often receive and answer questions from employees, parents and pupils about personal information held by the school, for example, where a member of staff is enquiring about the number of days they have been off sick. To ensure confidentiality, the individual must prove who they say they are, by making relevant checks, but the request is then dealt with in a routine, informal way.

School employees are encouraged to deal with informal requests for information with due care in such a manner.

Access to personal information

The DPA entitles anyone (of any age) about whom information is held, whether on computer or in paper files, to exercise their right of "subject access". This means that an individual can see everything a

school holds about them (with certain limited exceptions). These requests for information must be handled formally, owing to the additional legal responsibilities placed on the school by the DPA.

Where a pupil does not have sufficient understanding to make his or her own request, their parent (or person with parental responsibility) may make the request on their behalf. It is generally accepted that by the age of 12 the child is considered to have sufficient maturity to understand the nature of the request.

The individual can appoint an agent to make the request on their behalf. If they wish to appoint an agent, they need to complete an authorisation of agent form (see appendix 3) and provide proof of identity for the agent as well as for themselves.

To make a formal subject access request the individual should:

- complete a separate request in writing (a form is provided in appendix 1)
- give evidence to confirm identity (such as passport, birth certificate, driving licence or bank card)
- provide sufficient information to locate the information requested. Schools cannot, and by law are not obliged to, comply with a request such as "What information does the school hold about me?" or vexatious requests. However, schools should not ignore such a request, but ask the individual to provide more information to enable the request to be fulfilled
- pay a maximum fee of £10 (VAT exempt) (this is a discretionary charge)
- complete an authorisation of agent form and provide a suitable form of ID for the agent (if an agent has been appointed).

The individual has the right to:

- be told whether the school or someone else on its behalf is processing their personal information (processing includes holding the information but not doing anything with it)
- be given a description of the personal information; the purposes for which it is being processed, and those to whom the personal information is, or may be, disclosed
- be provided with a permanent copy of the information held *within 40 calendar days*, in an easy to understand form, (eg. any codes used need to be explained). If this is not possible, or 'disproportionate effort' is involved, or the individual agrees otherwise then a permanent copy of the information need not be provided – for example, the individual may agree to come into the school and look at electronic records on a PC instead. 'Disproportionate effort' is not defined and it must be judged on a case by case basis whether providing the information in permanent form would amount to disproportionate effort. Matters to consider include: the cost of providing the information; time taken to provide the information; how difficult it would be to provide the information. These matters will need to be balanced against the effect not providing a permanent copy could have on the individual
- be told the name of the source of the personal information held about them (except in limited circumstances)
- be informed about the logic involved if decisions which significantly affect them are made by fully automated means, for example for the purpose of evaluating matters about them, such as their performance at work. There are some exemptions to this rule.

In principle, individuals have a right of access to all of their personal information, although there may be some instances where information may be withheld. The main exemptions are:

- Information which may cause harm to the physical or mental health of the individual or a third party

- Information which may identify third parties (for example other pupils, although not teachers)
- Information which forms part of some court reports
- Information may also be withheld *if in that particular case* it would hinder the prevention and detection of crime, or the prosecution or apprehension of offenders if provided.

If you are unsure about the disclosure of information please contact Torbay Council's Information Governance Team for advice.

Processing a subject access request for personal information

On receipt of a formally made subject access request the school only has *40 calendar days* to provide the personal information requested.

Step 1
Check all the required documentation has been received (application form; authorisation of agent form, if applicable; suitable proof of identity; fee, if applicable, and sufficient detail to locate and supply the information requested).

Acknowledge receipt of the request.

Step 2
Locate the information relating to the request. Search manual records as well as all electronic records (including emails).

Make 3 exact copies of the information (photocopy manual records, print electronic records):
- copy one - should be kept as an untouched original
- copy two - is a working copy with any notes added as to why information has been redacted, or not disclosed
- copy three - the finalised redacted version, an exact copy of the information disclosed to the individual.

Step 3
Prepare the file(s) for disclosure to ensure it is disclosed in accordance with the DPA. This involves removing, or redacting, the information the individual is not entitled to under the DPA. The easiest way to redact is to edit the information with a black marker pen, so that when the redacted version is photocopied the redacted information cannot be seen.

In general the information that needs to be redacted is any personal information of which the individual is not the focus, for example, third party information. Also any information provided in confidence, or where there was an initial expectation that the information would not be revealed, should not be disclosed either.

Where information has been provided by a third party or by a Health Professional, always seek their consent prior to disclosing the information.

Step 4
Photocopy the redacted version and ensure the information cannot be seen through the black marker pen overwrites.

Step 5

Prepare a response letter to accompany the file and send the file by recorded delivery to ensure it is delivered to the individual. The envelope should be addressed as 'Private and Confidential'.

Step 6
Keep a log of the request, and any relevant information relating to it.

Access to educational records

The Education (Pupil Information) (England) Regulations 2000 provides *pupils and parents* with the right of access to 'educational records'. Educational records are the official records for which teachers are responsible and which relate to an individual who either is, or has been, a pupil at the school. However, it does not include information which is processed by a teacher *solely* for their own use.

An educational record is defined as any record of information which:

- is processed by or on behalf of the Governing body, or teacher of the school
- relates to any person who is or has been a pupil at the school
- originated from or was supplied by, or on behalf of:
    - an employee of the LEA which maintains the school
    - a teacher (other than information processed by a teacher solely for their own use)
    - other employee of the school (including an educational psychologist engaged by the governing body under a contract for services)
    - the pupil (to whom the record relates)
    - the parent of the pupil

It does not include information about the physical or mental health or condition of the individual, to which the Data Protection (Subject Access Modification) (Health) Order 2000 applies.

Pupils also have the right to be given a description of the personal data which makes up the record, together with details of the purposes their data is processed; sources of the data (if known); and the individuals or organisation to which the data may be disclosed (eg the Local Education Authority or the Department for Education & Skills).

Note: A very short period of 15 school days is allowed to respond to a request for access to educational records.

Parental rights to access educational records

Further to the subject access rights which can be exercised by parents acting on behalf of pupils, the Education (Pupil Information) (England) Regulations 2000 provide *parents* with an independent right of access to the official educational records of their children.

They are entitled to the same information in the educational record as pupils, but this right excludes information which does not form part of the official record.

As long as they have parental responsibility for the child, this right exists regardless of their living arrangements (ie the right exists even if they do not live with the child), unless there is a court order against them limiting this right.

This independent right means that pupils cannot prevent their parents from obtaining a copy of their school records.

Parents seeking to access their child's educational records do not have the right of redress under the DPA unless they are acting on behalf of their child.

When the information requested does not form part of an educational record, the right of access still applies but the usual subject access procedure must be followed.

See appendix 2 for a copy of the form to be used when a pupil or parent wishes to access educational records.

Fees for processing a subject access request for educational records

Upon request, the educational record must be made available for inspection free of charge. A fee may only be charged when a *hard copy* of the educational record is requested. The scale of charges for a hard copy of the educational record is based on the number of pages provided (see table below). Where information other than an official educational record is being requested, the maximum fee that may be charged is £10 in accordance with the DPA.

No. of Pages	**Maximum Fee**		**No. of Pages**	**Maximum Fee**
1-19	£1		100-149	£10
20-29	£2		150-199	£15
30-39	£3		200-249	£20
40-49	£4		250-299	£25
50-59	£5		300-349	£30
60-69	£6		350-399	£35
70-79	£7		400-449	£40
80-89	£8		500+	£50
90-99	£9			

Processing a subject access request for educational records

On receipt of a formally made request to access educational records, the school has *15 school days* to provide the information (the equivalent period for other types of personal records is up to 40 days under DPA).

In principle, pupils have a right of access to the whole of their educational records (as do parents with parental responsibility), although there may be some instances where information may be withheld. The main exemptions are:

- Information which may cause harm to the physical or mental health of the student or a third party
- Information which may identify third parties (for example other pupils, although not teachers)
- Information which forms part of some court reports

- Information may also be withheld *if in that particular case* it would hinder the prevention and detection of crime, or the prosecution or apprehension of offenders if provided.

The steps for dealing with a request for information held in educational records are the same as those for responding to a subject access request under DPA. See section 10.4 above for details.

Who should deal with any requests for personal information?

All requests for any personal information should be forwarded to the Head Teacher. Always take the name, address and telephone number of the enquirer so that the appropriate forms and information can be provided.

The Head Teacher should keep a copy of the information provided on the file for future reference.

It is the Head Teacher's responsibility to ensure that any exemptions applied when withholding information are in compliance with the terms of the legislation. If there is any doubt, always consult the Information Governance Team.

Compliance

Compliance with the legislation is the responsibility of all members of the school who process personal information.

All staff (including temporary workers) must be informed of their responsibilities under the DPA as soon as possible after starting work at the school. Further training must be provided to ensure levels of awareness remain high, particularly where staff have access to highly confidential or sensitive information and where information is regularly shared with others.

Pupils should have an awareness of the DPA and also understand that they have rights under it.

Criminal Offences

There are several offences under the DPA, which is why it is important that all members of staff fully understand their own responsibilities under the legislation, as well as those of the school.

Breach of the principles

The Information Commissioner has the power to serve an enforcement notice upon the school, if there is a contravention of any of the Data Protection Principles. Such a notice may be served on the school *or* an individual employee. Failure to comply with this notice, an information notice, or a special information notice will result in prosecution.

If an individual knowingly or recklessly commits a deliberate breach of the Act, or the breach occurs as a result of negligence and it contravenes school policy, then the Courts may well hold that individual personally liable.

Unauthorised disclosure, procurement and sale of information

The Act makes it an offence for a person who knowingly and recklessly, without the consent of the school:

- obtains or discloses personal information
- procures the disclosure to another person of the personal information

There are exceptions to liability for this offence eg. where it can be shown that the obtaining, procuring or disclosure was:

- necessary to prevent or detect crime
- required or authorised by law
- made by an individual acting in the reasonable belief that there was a legal right to do so
- made by an individual acting in the reasonable belief that the school would have consented if they had known about it, or
- justified as being in the public interest

It is a further offence to sell or offer personal information for sale that has been unlawfully obtained, or procured.

Enforced subject access

It is a strict liability offence to force or require someone to make a request to see a copy of their information, and to make them then give access to a copy of that information.

Notification offences

It is an offence for the school to process personal information without a current valid notification entry, and also to fail to notify the Commissioner of changes to the register entry.

Destruction of information

Personal information should be treated as confidential waste when it is destroyed. Different formats require different methods of destruction for example:

- Manual records (paper) - shred
- Floppy disks and CD's – snap or scratch
- Microfilm – incinerate or shred
- Hard drives of redundant PCs – wipe clean before disposal, or if that is not possible, destroy physically

Formatted: Bullets and Numbering

If using a third party company to destroy any personal information that third party must always supply a valid destruction certificate for the destroyed information.

Keep a record of the information that has been destroyed (including date of destruction, description of the information, and reason for destruction).

Glossary Of Terms

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 (eg. 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, 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.

Educational Record
Any record of information which:

- is processed by or on behalf of the Governing body, or teacher of the school
- relates to any person who is or has been a pupil at the school
- originated from or was supplied by, or on behalf of:
    - an employee of the LEA which maintains the school
    - a teacher (other than information processed by a teacher solely for their own use)
    - or other employee of the school (including an educational psychologist engaged by the governing body under a contract for services)
    - the pupil (to whom the record relates) or
    - the parent of the pupil

It does not include information about the physical or mental health or condition of the data subject. The Data Protection (Subject Access Modification) (Health) Order 2000 applies to this information.

Parent
Has the meaning given in the Education Act 1996, and includes any person having parental responsibility or care of a child.

Contacts

Torbay Council Information Governance Team:

Karen Jane Mitchell
Information Governance Manager
01803 207417
Karen.mitchell@torbay.gov.uk

Nikki Barron
Information Governance Assistant
01803 207467
Nikki.barron@torbay.gov.uk

appendices

Appendix 1 – Access to Personal Data Request Form

[School name and logo]

Access to Personal Data Request Form
Section 7 Data Protection Act 1998

You should complete this form if you want us to provide you with a copy of your personal data, which we hold about you or *your* educational record.

Please note you must send a fee of £10 before we can proceed with your enquiry under the Data Protection Act. Cheques should be made payable to [X].

We will endeavour to respond promptly to your request for *personal data* and in any event within 40 days of receipt of:

- this completed form
- satisfactory proof of identity
- £10 fee

We will endeavour to respond promptly to your request for your *Educational Record* and in any event within 15 school days of receipt of:

- this completed form
- satisfactory proof of identity
- fee (where applicable on request for a *copy* of your educational record)

Please tick the options that apply:

I am making this application for personal data about me (the Data Subject)	☐
I am requesting to *see* my Educational Record	☐
I am requesting a *copy* of my Educational Record (a fee may be required)	☐
I would like my agent to deal with my application on my behalf (I attach a signed authorisation of agent for subject access form)	☐

Data Subject Details Please provide details for the person you are requesting information about:

Title:		Date of Birth:	
Forename:		Surname:	
Address:			
Post Code:		Telephone Number:	

Please provide a description of the sort of personal data, which you are seeking together with any dates from which we should search. We reserve the right, in accordance with section 8(2) of the Act, not to provide you with copies of the information requested if to do so would take "disproportionate effort".

State how you would like the reply to this request to be dealt with:

Sent to your home address (as stated)	☐
Collected from the school (You must bring evidence to confirm your identity)	☐
Sent to your authorised agent (if appointed)	☐

If you specifically need the answers to the following, please tick the boxes

Why we are processing your personal data	☐
To whom your personal data may be disclosed	☐
The identity of the Data Controller	☐

Note: - if the information you request reveals details directly or indirectly about another person, we will have to seek the consent of that person before we can let you see that information. In certain circumstances we may not be able to disclose the information to you, in which case you will be informed promptly and given full reasons for that decision.

When you have received the requested information, if you believe that:

- The information is inaccurate or out of date; or
- We should no longer be holding that information; or
- We are using your information for a purpose of which you were unaware; or
- We may have passed inaccurate information about you to someone else; then

You should notify the Head Teacher/ Data Protection Officer at once, giving your reasons. The Head Teacher/ Data Protection Officer will then review the information and may amend your personal data in accordance with your wishes. Alternatively, the Head Teacher/ Data Protection Officer may notify you, giving reasons, as to why they believe the information held about you is in fact accurate and relevant and is being processed for fair and lawful purposes.

Please complete the following and return this form to:

The Head Teacher, [X] School, [address]

I confirm that I have read and understand the terms of this subject access form.

Signature:		Dated:	
Name (use block capitals):			

Appendix 2 – Access to Educational Records

[School name and logo]

Access to Educational Records under the Education (Pupil Information) (England) Regulations 2000

You will need to complete this form if you wish to access your child's (or child you have parental responsibility for) Educational Record.

	Please tick:
I am applying for a copy of the Educational Record of the Data Subject (I confirm I *am the parent / *have parental responsibility of the data subject (*please delete as appropriate).	☐

Data Subject Details Please provide details for the person you are requesting information about:

Title:		Date of Birth:	
Forename:		Surname:	
Address:			
		Post Code:	

Enquirer Details (if you are not the data subject) Please provide your own details here:

Title:		Date of Birth:	
Forename:		Surname:	
Address:			
Post Code:		Telephone Number:	

I declare I *am the parent / *have parental responsibility for the above child and accept you may need to make further enquiries to validate this (*delete as appropriate). I have provided suitable proof of identity with this application.

Signature:	
Name (use block capitals):	
Date:	

Appendix 3 – Authorisation of Agent Form

[School name and logo]

Authorisation of Agent for Subject Access
Data Protection Act 1998

This application for Subject Access is made on behalf of:

DATA SUBJECT (to be completed and signed by the data subject):

Title:		Date of Birth:	
Forename:		Surname:	
Address:			
		Post Code:	

I am the above-named person and authorise Torbay Council to give the information requested in this application to my agent whose name and address are given below.

Signature of person giving authority:	
Name (use block capitals):	
Date:	

AGENT:

Title:		Date of Birth:	
Forename:		Surname:	
Address:			
Post Code:		Telephone Number:	

What is your relationship with the data subject?

I declare that I make this application on behalf of and solely in the interest of the named Data Subject. To ensure confidentiality I accept that you may need to make further enquiries to validate this authorisation. I have provided suitable proof of identity with this application.

Signature of agent:	
Name (use block capitals):	
Date:	

Appendix 4 – Subject Access Request Section 29

[School name and logo]

Subject Access Request – Section 29
Made under the Data Protection Act 1998

Please complete the following and return to:

Head Teacher/Data Protection Officer
School
Address

I am making enquires which are concerned with:

• The prevention and detection of crime	☐
• The apprehension or prosecution of offenders	☐

(Tick the appropriate option)

Nature of enquiry:

The information sought is needed to:

and possibly for other crime enquiries and administration purpose(s). I confirm that the personal data requested are required for this purpose/those purposes, and failure to provide the information, in my view, would be likely to prejudice that/those purposes.

This enquiry is confidential and should not be communicated to the data subject

Name:			Tel No:	
Authority:			Position:	
Address:				
Signed:			Date:	
	(Block capitals)			
Countersigned:			Position:	
Name:			Date:	
	(Block capitals)			

Appendix 5 – Consent for children under 12

[School name and logo]

Consent to use images of children under the age of 12
Data Protection Act 1998

Name of Child:	
Name of parent or guardian:	

From time to time we may take photographs of children at the school to use in our school prospectus or other printed publications we produce. [Theses images may also be used on our website www.xxxxxxxx].

To comply with the Data Protection Act 1998, we need your permission before we can take any images of your child. Please answer the questions below by ticking the relevant box, sign the form and return to [X]

Please tick:

	YES	NO
May we use your child's photograph in the school prospectus and other printed publications that we produce for promotional purposes?	☐	☐
May we use your child's image on the school website www.xxxxxxxxxx ?	☐	☐

Please note that websites can be viewed throughout the world, not just in the United Kingdom where UK law applies. Please also note the conditions for using these images on the back of this form.

I have read and understood the conditions of use on the back of this form.

Signature of parent or guardian:		Date:	
Name (block capitals):			

CONDITIONS OF USE

- This form is valid for [X] years from the date of signing/ for this project only. Your consent will automatically expire after this time.
- We will not re-use any images after the period of consent expires / after the project is completed.
- We will not include personal e-mail or postal addresses, or telephone or fax numbers on our website.
- We will not include details or full names (which means first name and surname) of any child or adult in an image on our website without good reason. For example, we may include the full name of a competition prize winner if we have their consent.
- If we use images of individual children, we will not use the name of that child in the accompanying text or photo caption without good reason. And if a child is named in the text, we will not use the image of that child to accompany the article without good reason (as in the example given above).
- We may use group or class photographs with very general labels, such as “a science lesson” or “art class”
- We will only use images of children who are suitably dressed, to reduce the risk of such images being used inappropriately.

Appendix 6 – Consent for using images of data subject's over 12

School name and logo

Consent to use images of data subject's over the age of 12
Data Protection Act 1998

Name of data subject:	

From time to time we may take photographs of children at the school to use in our school prospectus or other printed publications we produce. [Theses images may also be used on our website www.xxx].

To comply with the Data Protection Act 1998, we need your permission before we can take any images of you. Please answer the questions below by ticking the relevant box, sign the form and return to [X]

Please tick:

	YES	NO
May we use your photograph in the school prospectus and other printed publications that we produce for promotional purposes?	☐	☐
May we use your image on the school website www.xxx	☐	☐

Please note that websites can be viewed throughout the world, not just in the United Kingdom where UK law applies. Please also note the conditions for using these images on the back of this form.

I have read and understood the conditions of use on the back of this form.

Signature of data subject:		Date:	
Name (block capitals):			

CONDITIONS OF USE

- This form is valid for [X] years from the date of signing/ for this project only. Your consent will automatically expire after this time.
- We will not re-use any images after the period of consent expires / after the project is completed.
- We will not include personal e-mail or postal addresses, or telephone or fax numbers on our website.
- We will not include details or full names (which means first name and surname) of any child or adult in an image on our website without good reason. For example, we may include the full name of a competition prize winner if we have their consent.
- If we use images of individual children, we will not use the name of that child in the accompanying text or photo caption without good reason. And if a child is named in the text, we will not use the image of that child to accompany the article without good reason (as in the example given above).
- We may use group or class photographs with very general labels, such as “a science lesson” or “art class”
- We will only use images of children who are suitably dressed, to reduce the risk of such images being used inappropriately.

Appendix 7 – Confidentiality Agreement

[School name and logo]

Data Protection Confidentiality Agreement

- [X] school has provided the information in confidence to you for the purpose of [X] and must only be used for the stated purpose. The information remains the property of [X] school and must be returned or destroyed on completion.
- The information supplied constitutes personal data and must be processed in accordance with the principles of the Data Protection Act 1998.
- Appropriate measures must be taken to prevent the unlawful or unauthorised processing of the personal information supplied.
- On agreed completion, all copies of information should be returned or destroyed (as confidential waste) and deleted from your systems (including back up copies). Certification of the return or destruction of information is requested by completing and returning the form below.