Holy Trinity C. E. (A) Primary School, Cuckfield
Data Protection Policy

General Statement
The Headteacher and Governors of Holy Trinity CE(A) Primary School intend to comply fully with the requirements and principles of the Data Protection Act 1998. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities under this policy.

Fair Obtaining
The School undertakes to obtain and process personal data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' rights of access. Information about the use of personal data is printed on the appropriate collection form, if details are given verbally the person collecting will explain the issues before obtaining the information.

Registered Purposes
The Data Protection Registration entries for the School are available, by appointment, for inspection in the school office. Explanation of the codes and categories entered is available from the Bursar, who is the person nominated to deal with Data Protection issues in the school. Registered purposes covering the data held at the school are listed on the school's Registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subjects' consent.

Data Integrity
The School undertakes to ensure data integrity by the following methods:

Data Accuracy
Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the School of a change of circumstances their record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, the School will immediately mark the record as potentially inaccurate or 'challenged'. We shall try to resolve the issue informally but if this is not possible, any disputes will be referred to the Governing Body for their deliberation.

If the problem is not resolved at this stage independent arbitration may be sought by either side. Until resolved, the challenged marker will remain and all disclosures of the affected information will contain both versions of the information. In order to prevent such problem areas we shall provide data subjects with opportunities to check their data accuracy and request amendments.

Data Adequacy and Relevance
Data held about people will be adequate, relevant and not excessive to the purpose for holding the data. In order to ensure compliance with this principle, the School Admin Officers with responsibility for data input and maintenance will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

Length of Time
Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Bursar and School Admin Officers, with appropriate guidance, to ensure obsolete data are properly erased.

Subject Access
The Data Protection Act extends to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received in respect of a pupil, the school's policy is that :

- Requests from parents/carers of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.
- Requests from pupils will be referred to the child's parents/carers.

Processing Subject Access Requests
Students/parents should ask for the Subject Access form available from the School Office and staff should use the Staff Request form available from the Headteacher. Completed forms should be submitted to the Bursar. Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, indicating the date of receipt, data subject's name, name and address of requester (if different), type of data required (e.g. Student Record, Personnel Record) and planned date of supplying the information (not more than 40 days from the request date).

Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be the date on which sufficient information has been provided.

Authorised Disclosures
In general, the School will only disclose data about individuals with their consent (for pupils at the school consent will be obtained from the parent/carer). However, there are circumstances under which the school's authorised officer(s) will reveal data without express consent. The schools' authorised officers are the Headteacher, Assistant Headteacher/Child Protection Officer.

These circumstances are intentionally limited to :

- Pupil data disclosed to authorised recipients in respect of education and administration necessary for the school to perform its legitimate duties and obligations.
- Pupil data disclosed to authorised recipients in respect of a child's health, safety and welfare
- Pupil data disclosed to parents in respect of their children's progress, attendance, attitude and general demeanour within, and in the vicinity of, the school
- Staff data disclosed to the relevant authority in respect of payroll and schools' staff administration

- Other disclosures as may prove unavoidable, for example where an incidental disclosure occurs when an engineer is fixing the computer systems. In such cases, the engineer will sign a document to promise NOT to disclose such data outside the school. Education Authority IT Liaison/Support Officers are professionally bound not to disclose such data.

Any request for disclosure of information will be referred to the schools authorised officers. Only authorised and properly instructed staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare workers must be made available only if the staff member **needs to know** the information for their work within the school.

Data and Computer Security
Holy Trinity CE(A) Primary School undertakes to ensure security of personal data by the following general methods - (for security reasons we cannot reveal precise details in this document) :

Physical Security
Appropriate building security measures are in place, such as alarms, window bars, lockable cabinets, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the computer room. Disks, tapes, printouts and files are locked away securely when not in use. Visitors to the school are required to sign in and out and are, where appropriate, accompanied.

Logical Security
Security software is installed on all computers containing personal data, only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (i.e. security copies are taken) regularly. Filing cabinets should be kept locked when the room is unattended.

Procedural Security
Access to computer records is restricted to identified personnel only. All staff are trained and instructed in their Data Protection obligations and their knowledge updated as necessary. Computer printout and source documents are always shredded before disposal.

Overall security policy is determined by the Headteacher in conjunction with the Governing Body and will be monitored and reviewed as appropriate and whenever a major security breach or loophole is apparent. Any queries or concerns about security of data within the school should be brought to the attention of the Headteacher.

Individual members of staff can be liable in law under the terms of the Act. They may also be subject to damages claims from persons harmed as a result of inaccuracy, unauthorised use or disclosure of their data. Any deliberate breach of this Data Protection policy will be treated as a disciplinary matter and serious breaches of the Act may lead to dismissal.

Enquiries
Further information about the School's Data Protection Policy is available from the Bursar and general information about the Data Protection Act can be obtained from the West Sussex County Council: http://schools.westsussex.gov.uk/Services/3163

Established: Finance Committee November 2012
Reviewed : January 2015, January 2017, October 2017

Appendix

Guidance from WSCC: Data Protection Information for Schools

The Data Protection Act 1998 came into force on 1 March 2000. It regulates the holding and processing of personal data, that is, information relating to living individuals which is held either on computer or in some cases in manual form.

The Act gives legally enforceable rights to individuals (data subjects) and places obligations on those who control the manner and the purpose of the processing of personal data (data controllers). Data controllers must notify the Commissioner of the details of their processing (details of which are published by the Commissioner in the register of notifications).

Data controllers must also comply with 8 data protection principles which together form a framework for the proper handling of personal data. Please see attached file below for further details.

Should you have any queries regarding Data Protection please contact the WSCC Legal Services Schools Helpline on 03302 222738.

Data Protection

1.1 The Data Protection Act 1998 (the Act) came into force on 1 March 2000. It regulates the holding and processing of personal data, that is information relating to living individuals, which is held either on computer or in manual form. Personal data can consist of paper files, CCTV images and photographs.

1.2 The school/college is a Data controller and must:

a) Notify the Information Commissioners Office (ICO) (see paragraph 2 below)
b) Comply with the eight data protection principles which together form a framework for the proper handling of personal data.

Registering your school/Notification under the Act.

2.1 The school should make one notification to the ICO on behalf of the governing body and head teacher in the school's name.

2.2 An application can be made either via the Commissioner's website (www.ico.gov.uk), or by telephoning the Notification Department (01625 545740). There is a standard notification template, which has been designed to cover schools activities (templates are available for private schools, and for community, foundation, voluntary-controlled and voluntary-aided schools).

2.3 The ICO sends renewal notices annually at which stage it is appropriate to review the notification to ensure it includes any new category of processing being undertaken.

3. The eight principles of data protection are:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.

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 for the rights and freedoms of data subjects in relation to the processing of personal data.

4. Data Subjects' rights

4.1 Right to know

Data subjects have the right to know what data is held about them, who is collecting it, for what purpose it is collected and who will see it. Schools should provide this information when collecting personal data. Schools may wish to use the "privacy notice" on forms asking for personal data to ensure this requirement is satisfied.

4.2 Right of access to personal data

See paras 5 and 6 below.

4.3 Right to prevent processing causing damage or distress

Subject to certain exemptions, data subjects have the right to serve a notice on data controllers requiring them to stop processing personal data in a way which is likely to cause substantial unwarranted damage or distress to that data subject or another.

4.4 Right to correct inaccurate data

Data subjects may also apply for a court order to require the data controller to rectify, block, erase or destroy inaccurate data about the data subject. Schools should therefore ensure that they have procedures in place to respond to any requests to amend inaccurate data.

5. Publication of schools' exam results

5.1 Objections to publication

Publishing examination results is a common and accepted practice. However, schools do have to act fairly when publishing results. Schools should ensure that all pupils and parents know that results are intended to be published and how they will be published. Schools do not have to gain the written consent of pupils and parents before publishing exam results.

5.2 Notification

Schools planning to publish exam results should ensure that disclosures to the media are included in their notifications when they register.

5.3 Privacy notices

Schools planning to publish exam results should ensure that disclosures to the media are included in their privacy notices.

6. Disclosures (extracts from ICO technical guidance note 'Access to pupils' information held by schools in England)

6.1 Requests for personal data by Pupil/Parent

What rights exist for access to a pupil's personal information?

There are two distinct rights to information held by schools about pupils.

1. The subject access right – under the Act a pupil has the right to a copy of their own information. In certain circumstances requests may be made by a parent on behalf of their child.
2. Rights to the educational record – under the Education (Pupil Information) (England) Regulations 2005, (he Regulations), a parent has the right to access their child's educational record.

Under the subject access right parents will only be able to see all the information about their child when the child is unable to act on their own behalf or gives their written consent.

At what age can a child make their own subject access request?
The Act does not specify an age at which a child can make their own request for access to their information. When a request is received from a child for access to their own information, those responsible for responding should take into account whether:

- the child wants their parent (or someone with parental responsibility for them) to be involved in the request; and
- the child properly understands what is involved in making the request and the type of information they will receive.
-

As a general guide, a child of 12 or older is expected to be mature enough to understand the request they are making.

Can any other information be withheld?

1. Information about another person (including a parent) should not be disclosed without consent of that person.
2. Information about the data subject where:

- information might cause serious harm to the physical or mental health of the pupil or another individual
- the disclosure would reveal a child is at risk of abuse
- information contained in adoption and parental order records
- information given to a court in proceedings under the Magistrates' Courts (Children and Young persons) Rules 1992
- copies of examination scripts
- providing examination marks before they are officially announced
- legal advice which is protected by legal professional privilege.

What are the timescales for dealing with requests?
Requests for information from pupils, or parents, for information that contains, wholly or partly, an educational record must receive a response within 15 school days.
Unless a parent simply asks to see the official educational record under the Regulations, schools and authorities are entitled to receive any fee first (see ICO technical guidance notes).

Most requests for information are likely to ask for at least some information in the educational record. However, should a subject access request be made just for personal information outside the educational record, a response must be made promptly and at most within 40 calendar days. However, the 40 days does not begin until after the fee and any further information about identity or the location of the information is received.

6.2 Requests from police/fraud office
Section 29(3) of the Act allows disclosure of personal data to the police where it is necessary for the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of any tax or duty or similar. The police should be able to show that if the school does

not disclose the information, the above purposes would be prejudiced. The police should make the request in writing on headed paper and the school should check that the individual making the request is indeed from the police/ fraud office. The sort of information the police usually require is the current address of a child's parents.

6.3 Court orders for disclosure
Schools should refer such requests, which may come from the police, the Crown Prosecution Service or the defence to a court case, to the Legal Services Unit at West Sussex County Council.

6.4 Education agencies
Disclosing data to education agencies should be covered in the schools 'privacy notice'.

6.5 Other third parties
The general rule is that personal data should not be disclosed to these third parties unless the school has the consent of the data subject or their parent.

7. Best Practice on disclosure

- Always check each page of a file before disclosure to ensure that there is no information about another person in it.
- If there is information about another person in it redact that information. If this is not possible because the information is inextricably linked then the Act in section 7(4) and 7(6) directs you to seek consents or disclose if it is reasonable in all the circumstances to do so.
- Do not share personal data with anyone other than the data subject without consent of the data subject unless one of the conditions in schedule 2 DPA is satisfied. (see schedule 2 annexed)
- Do not share sensitive personal data with anyone other than the data subject without consent of the data subject unless one conditions in schedule 2 and one condition in schedule 3 is present. (see schedule annexed).
- Take greater care when processing sensitive personal data: race, political opinion, religious belief, TU membership, physical or mental health, sexual life, commission of offences, criminal proceedings or sentences.
- Keep a record of disclosures.

8. Penalties for non compliance with the Data Protection Act
There are various criminal offences created by the Act, which can be committed by the school or by a member of staff, including:

- Failure to register/notify
- Procuring and selling offences

For further information, please contact the WSCC Legal Services Schools Helpline on 03302 222738.

8. Paying for information

Information published on our website is free.

Please also refer to the Freedom of Information Policy.

Single copies of information covered by this publication are provided free unless stated otherwise. If your request means that we have to do a lot of photocopying or printing, or pay a large postage charge, or is for a priced item such as some printed publications or videos we will let you know the cost before fulfilling your request.