St Stephen's CEVA Primary School, Bath

Information And Communications Technology (ICT) Policy

Note: Includes following policies:

- Data Protection (statutory)
- e-Safety
- Using St Stephen’s Computer Systems

Policy name:	Information And Communication (ICT)		
Policy type:	Policy (Data Protection: Statutory (B))		
Next review date:	01/sep/2015		
Prepared by:	IT	Date:	dd/mmm/yyyy
Approved by:	Full Governors Board	Date:	dd/mmm/yyyy
Filename:	ICT Policy (CURRENT).docx		
Document version:	1.3		

1 ICT Vision

All pupils at St. Stephen’s will experience regular and high quality teaching in ICT. They will have the opportunity to select and use ICT to support their learning and extend their communication skills.

Through training, staff will be confident in delivering the ICT curriculum and should be competent in teaching the other aspects of the National Curriculum through ICT (embedding ICT).

Both staff and pupils should be able to use the Internet effectively to aid teaching and learning.

2 The Breadth of ICT

Information and Communications Technology is concerned with storing, processing and presenting information by electronic means. ICT consists of all technical means used to handle information and aid communication, including computer and network hardware, as well as necessary software. In other words, ICT consists of IT as well as telephony, broadcast media, and all types of audio and video processing and transmission.

3 The Use of ICT in Learning and Teaching

ICT can be considered as a subject in its own right and a tool to support other subjects.

3.1 The Curriculum

At St. Stephen’s we aim to give all pupils a good grounding in ICT capability by:-

- Developing flexibility and openness of mind necessary to adjust to, and take advantage of, the ever-quickening pace of technological change, whilst being alert to the ethical implications and consequences for individuals and society.
- Enriching and extending learning throughout the curriculum, using the technology to support collaborative working, independent study and reworking of initial ideas, as well as to enable pupils to work at a more demanding level by avoiding some routine tasks.
- Helping children to acquire confidence and pleasure in using ICT, to become familiar with some every day applications and to be able to evaluate the technology's potential and limitations.
- Harnessing the power of the technology to help pupils with special educational needs or physical handicaps, to increase their independence and develop their interests and abilities.

We aim to give pupils:-

- The knowledge about applications of IT and about IT tools such as word processors, spreadsheets, databases and software for processing sounds and images
- The skill to use appropriate IT tools effectively
- An understanding of the new opportunities IT provides

- Knowledge of the effects and limitations of IT
- A good understanding of e-Safety

Pupils will be given the opportunity to:-

- Handle text
- Handle data
- Explore simulations
- Control systems
- Explore the creative arts

3.2 Continuity and Progression

Progress in IT is recorded for groups of pupils. Internal IT records for groups of pupils are kept and forwarded to the next class teacher. Each teacher will have a good software toolbox with software appropriate to the children's needs.

At Key Stage 2, samples of children's work are stored on the P: drive.

For Reception and Key Stage 1 it may not always be practical to keep samples of work, but observations and discussions are recorded.

4 Communication

A separate communications policy exists, which covers school communications in general, and includes the use of IT as a tool for communication.

5 Safe use of equipment

Instructions for the use of ICT equipment and systems form Appendix A of this policy.

Children are not to move heavy equipment around the school. They may load software but should not be given the responsibility of plugging in and switching machines on without a member of staff present.

Food and drink are not to be consumed near ICT equipment.

It is the responsibility of staff to ensure that classroom ICT equipment is stored securely, cleaned regularly and that they or their class leave the ICT Suite clean and tidy after use.

Staff should ensure that the children are seated at the computers comfortably and be aware of the dangers of continuous use (e.g. eye/wrist strain etc).

An adult should always supervise children when they are accessing information via the Internet. The service provider does filter information but staff are ultimately responsible for information accessed by pupils.

6 e-Safety

e-Safety guidance forms Appendix B of this policy.

7 Data Protection

Data protection forms Appendix C of this policy.

8 Equipment

The availability of appropriate hardware and software is regularly reviewed by the It committee and a hardware and a software inventory is kept and maintained by the ICT support provider (Smooth IT).

9 Staff Training and Professional Development

All staff will be given equal opportunities to expand their working knowledge of ICT. The ICT Co-ordinator produces an action plan each year, outlining the targets for that year.

Staff training needs will be met by:

- Auditing staff skills and confidence in the use of ICT regularly
- Arranging internal or external training for individuals as required
- The ICT Co-ordinator should attend courses and support and train staff as far as possible
- Regular Staff Meeting time dedicated to ICT

A. Appendix A: Using St. Stephen's Computer Systems

This part of the policy covers the use of IT equipment and systems. It sets out your responsibilities when using these systems. For the purposes of this policy the term PC will be used to mean all desktop or handheld devices designated for your use (whether shared or not).

1 Equipment

Only IT equipment listed in the School inventory may be used and no third party equipment (including wireless equipped systems) may be connected to IT networks or systems except with the approval of the Headteacher and ICT support provider (Smooth IT).

Computer systems supplied by the School must not be tampered with or modified in any way. Staff should not attempt to repair or alter computer equipment or install additional equipment themselves.

All desktop computer systems, printers and other peripherals must be shut down when not in use at the end of each working day, or if they are going to be left unused for a prolonged period during the day. This reduces power use and improves security.

All ICT equipment and systems supplied to staff are the property of St. Stephen's School. You should remember at all times that these systems are intended to be used primarily for School purposes.

When a member of staff leaves the School, any computer system and user rights put in place specifically for that staff member will be returned to the default arrangements for that system.

2 Software

Do not use any software on your PC other than that provided by the School or that which you have authorisation from the ICT support provider (Smooth IT).

2.1 Licensing

Software issued by the School for your use is licensed to the School and is subject to licensing agreements controlling its use. Only legally compliant licensed software may be used on the School's IT systems. It is illegal to make copies or distribute the software that you use in the course of your duties.

3 Copyright protection

St. Stephen's respects the copyright of those involved in creating and disseminating copyright material, such as music, films, software, and other literary, artistic and scientific works.

Users shall not:

- Make, store, transmit or make available unauthorised copies of copyrighted material on (School) systems, equipment or storage media.
- Download, upload, store or make available unauthorised copies of copyrighted material via the internet using school systems, equipment or storage media.
- install or run peer-to-peer 'file-sharing' software or operate a peer-to-peer index or server on school systems or equipment.

Any questions as to whether an employee or pupil may copy or use copyrighted material in ways covered by this policy should be raised with the Headteacher before proceeding.

4 Laptops

In order to mitigate the risk of the loss of sensitive or personal data that could arise from the theft or loss of a School laptop the following provisions must be followed:

- In accordance with the Data Protection Act no sensitive data relating to pupils or staff is to be held on the 'C' drive of a laptop. Any such information should be held on the secure section of each member of staff's data pen in accordance with appendix c (data protection).
- All School laptop users must use a 'power on' password on their laptop.

B. Appendix B: E-Safety

As E-safety is an important aspect of strategic leadership within the school, the Head and the Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The school's ICT Co-ordinator will also act as e-safety Co-ordinator and all members of the school community have been made aware of who holds this post. It is the role of the co-ordinator to keep abreast of current issues and guidance through the relevant organisations.

1 Learning and Teaching

Why is use of the Internet important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning and teaching. It is an essential element in 21st Century life and therefore access to the Internet should be an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

However, whilst exciting and beneficial both in and out of the context of education much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At St. Stephen's we understand the responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

2 Internet Access

Pupils will be taught to Evaluate Internet Content.

The school will ensure that the use of Internet derived materials by staff and pupils should be lawful and appropriate. Pupils will be taught to be critically aware of the materials they read and will be shown how to validate information before accepting its accuracy.

2.1 Use of Internet Facilities

Internet access should not compromise St. Stephen's CE Primary School's information and computer systems nor have the potential to damage St. Stephen's CE Primary School's reputation.

Users shall not visit internet sites, make, post, download, upload or pass on material, remarks, proposals or comments that contain or relate to:

- child pornography
- pornography
- promoting discrimination in any way
- promoting racial or religious hatred

- promoting illegal acts

Incidents that appear to involve deliberate access to Web sites, newsgroups and online groups that contain the following material will be reported to the police:

- images of child abuse (images of children, apparently under 16 years old) involved in sexual activity or posed to be sexually provocative
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in the UK

If inappropriate material is accessed accidentally, users should immediately report this to the Headteacher so that this can be taken into account in monitoring.

Users shall not:

- Use St. Stephen's CE Primary School facilities for running a private business
- Visit sites that might incur liability on the part of St. Stephen's CE Primary School or adversely impact on the image of St. Stephen's CE Primary School
- Reveal or publicise confidential or proprietary information, which includes but is not limited to: financial information, personal information, databases and the information contained therein, computer/network access codes and business relationships.
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network work traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet.
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate.

2.2 Monitoring

Our service provider – South West Grid for Learning (SWGfL) – will monitor and audit the use of the Internet at school to see whether users are complying with the policy. Any potential misuse identified by the SWGfl will be reported to the school and/or relevant organisation.

It is up to individual staff to monitor the use of the Internet at home and ensure that they are complying with the policy. Any misuse noted by a member of staff should report to the ICT co-ordinator and/or relevant organisations.

2.3 Filtering

The SWGfL provides Internet filtering powered by RM SafetyNetTM Plus. This service is designed to protect children by filtering out material found to be inappropriate for use in the education environment. However, it is essential that teachers ensure the pupils are properly supervised when using the Internet.

If staff or pupils discover an unsuitable site, it must be reported to the e-Safety officer

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable

2.4 Reporting Abuse

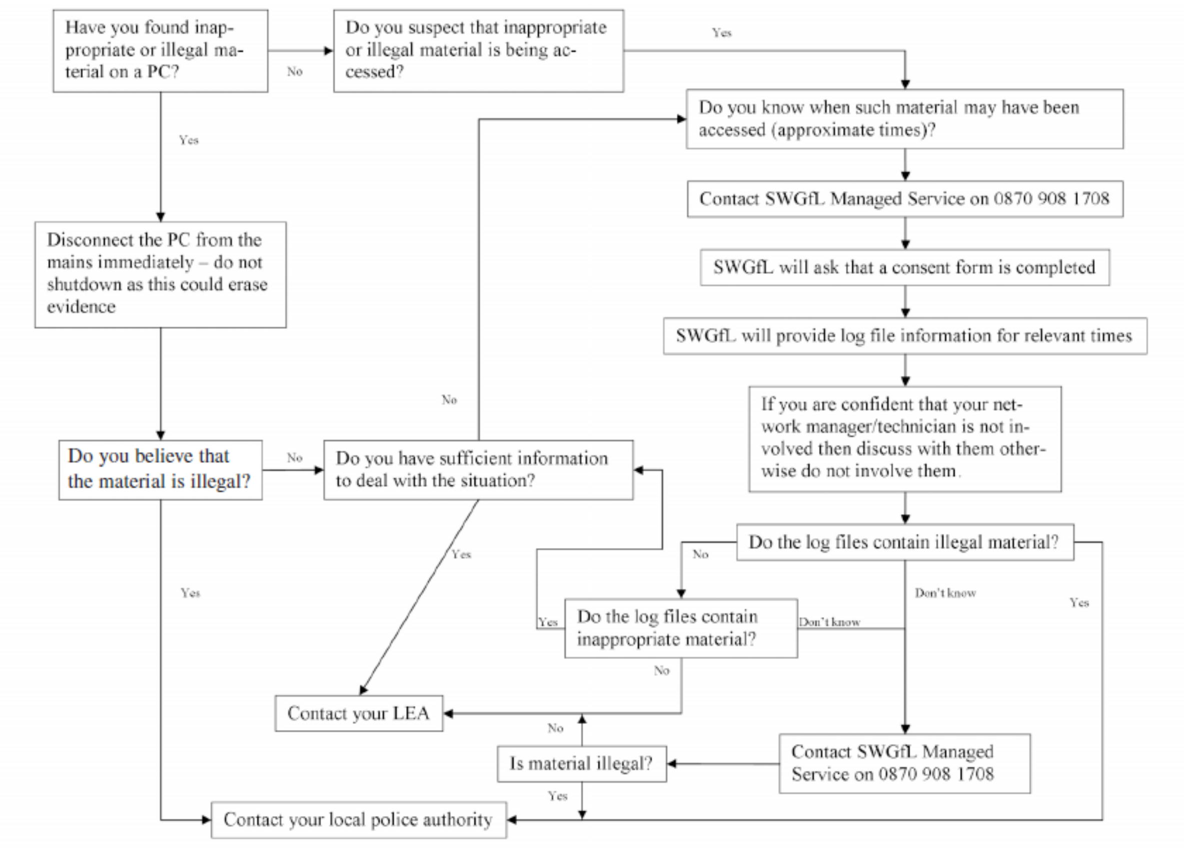
All abuse complaints must be logged in writing or, for legal reasons, they cannot be acted upon. An email reporting the complaint should then be sent to abuse@swgfl.org.uk stating the nature of the complaint. If the abuse is in the form of an email, then copies of the email, including full headers should be sent to the above address.

2.5 Children

Relevant points regarding safe Internet use will be communicated to our pupils on a yearly basis at an appropriate level. Relevant reminders will be made when necessary.

2.6 Internet Safety Protocol

The following Internet Safety Protocol is designed to be a point of reference in the event that the Internet is used to access (or on the suspicion of access) inappropriate or illegal material. If a teacher feels that such material is being accessed, they should follow the protocol, they should not involve any other members of staff. SWGfL will manage any situations both in, and with, confidence.


Have you found inappropriate or illegal material on a PC?
No
Do you suspect that inappropriate or illegal material is being accessed?
Yes
Do you know when such material may have been accessed (approximate times)?
Yes
Contact SWGfL Managed Service on 0870 908 1708
SWGfL will ask that a consent form is completed
Disconnect the PC from the mains immediately – do not shutdown as this could erase evidence
SWGfL will provide log file information for relevant times
No
If you are confident that your network manager/technician is not involved then discuss with them otherwise do not involve them.
Do you believe that the material is illegal?
No
Do you have sufficient information to deal with the situation?
Yes
Do the log files contain illegal material?
No
Yes
Don't know
Yes
Yes
Do the log files contain inappropriate material?
Don't know
No
Contact your LEA
No
Is material illegal?
Contact SWGfL Managed Service on 0870 908 1708
Yes
Contact your local police authority

Police Telephone Number: 0845 4567000

3 Information System Security

The School ICT systems capacity and security will be reviewed regularly. The virus protection will be updated regularly.

4 Email

- Pupils may only use approved e-mail accounts on the school system
- Pupils must immediately tell an adult if they receive offensive mail
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- The forwarding of chain letters is not permitted

5 Published content on the School Website

The contact details on the Website are the school address, email and telephone number. Staff or pupil personal information will not be published.

The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

6 Publishing Pupil's Images and Work

- Signed permission from parents or carers will be obtained before photographs of pupils are published on the school website or learning platform
- Parents/carers may withdraw permission, in writing, at anytime.
- Photographs that include pupils will be selected carefully
- Pupils' full names will not be used anywhere on the website or learning platform

7 Social Networking and Personal Publishing

- The school will block / filter access to social networking sites
- Newsgroups will be blocked unless a specific use is approved. Pupils will be advised never to give out personal information
- Pupils and parents will be advised that the use of social networking spaces outside of school is inappropriate for primary aged pupils
- In the event of parents / carers wanting to take photos for their own personal use, the school will demonstrate its protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites

8 Managing Video-Conferencing

When it is introduced to school, video-conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet

Video-conferencing will be appropriately supervised for all pupils

9 Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The use of portable media such as memory sticks and CD ROMS will be monitored closely as potential sources of computer virus and inappropriate material.
- Pupils are discouraged from bringing personal mobile devices/phones to school. Any phones that are brought to school should be turned off and kept in the pupils' bags.
- The sending of abusive or inappropriate text messages outside school is forbidden.
- Staff will use a school phone where contact with pupils is required.
- Staff should not use personal mobile phones during designated teaching sessions

10 Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1988. More detail can be found at appendix c (data protection).

11 Handling e-Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the Head teacher
- Complaints of a child protection nature must be dealt with in accordance with the school child protection procedures

12 Communication of Policy

12.1 Pupils

- Rules for Internet Access will be posted in all networked rooms
- Pupils will be informed that Internet use will be monitored

12.2 Staff

- All Staff will be given this Policy and its importance explained
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- A laptop issued to a member of .staff remains the property of the school. Users of such equipment should therefore adhere to school policy, both in and out of school.

12.3 Parents

Parents' attention will be drawn to this policy in newsletters and on the school website

C. Appendix C: Data Protection

The Governing Body of the school has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Headteacher and Governors of this School intend to comply fully with the requirements and principles of the Data Protection Act 1984 and the Data Protection Act 1988. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

1 Enquiries

General information about the Data Protection Act can be obtained from the Data Protection Commissioner (Information Line 01625 545 745, website www. dataprotection.gov.uk).

2 Obtaining and processing data

St. Stephen's CE VA Primary School undertakes to obtain and process 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' right 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.

3 Registered purposes

The Data Protection Registration entries for the School are available for inspection, by appointment, at the school office. Explanation of any codes and categories entered is available from the Headteacher 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 subject's consent.

4 Data integrity

The school undertakes to ensure data integrity by the following methods:

4.1 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 computer record will be updated as soon as is practicable.

Where a data subject challenges the accuracy of their data, the School will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Governing Body for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

4.2 DATA ADEQUACY AND RELEVANCE

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the School will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

4.3 LENGTH OF TIME

Data held about individuals will not be kept for longer than necessary for the purposes registered.

4.4 SUBJECT ACCESS

The Data Protection Acts extend 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 from a pupil, the school's policy is that:

- Requests from pupils will be processed as any subject access request as outlined below and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.
- Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.
- Requests from parents in respect 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.

5 PROCESSING SUBJECT ACCESS REQUESTS

Requests for access must be made in writing using the Data Subject Access form (at the end of this document). Completed forms should be submitted to the Headteacher. Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (eg Student Record, Personnel Record), and the planned date of supplying the information (normally 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.

Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations.

6 AUTHORISED DISCLOSURES

The School will, in general, only disclose data about individuals with their consent. However there are circumstances under which the School's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.
- Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.
- Staff data disclosed to relevant authorities eg in respect of payroll and administrative matters.
- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the school. Officers and IT personnel writing on behalf of the LEA are IT liaison/data processing officers, for example in the LEA, are contractually bound not to disclose personal data.
- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who need to know the information in order to do their work. The school will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child abuse.

A "legal disclosure" is the release of personal information from the computer to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.

An "illegal disclosure" is the release of information to someone who does not need it, or has no right to it, or one which falls outside the School's registered purposes.

7 DATA AND COMPUTER SECURITY

St. Stephen’s CE VA Primary School undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed).

7.1 PHYSICAL SECURITY

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

7.2 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 regularly.

7.3 PROCEDURAL SECURITY

All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal.

Overall security policy for data is determined by the Headteacher and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. The School's security policy is kept in a safe place at all times.

Any queries or concerns about security of data in the school should in the first instance be referred to the Headteacher.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as a disciplinary matter, and serious breaches could lead to dismissal.

8 Access to personal data request

Data Protection Act 1998 Section 7.

Enquirer's Surname: …………………………

Enquirer's forenames: ……………………………..

Enquirer's Address:

……………………………………………………………………………

……………………………………………………………………………

……………………………………………………………………………

Enquirer's Postcode: ……………………………

Telephone Number: ……………………….

Are you the person who is the subject of the records you are enquiring about? (i.e. the "Data Subject")?

YES / NO (delete as required)

If NO,

Do you have parental responsibility for a child who is the "Data Subject" of the YES / NO records you are enquiring about?

If YES,

Name of child or children about whose personal data records you are enquiring

……………………………………………………………………..

……………………………………………………………………..

……………………………………………………………………..

……………………………………………………………………..

Description of Concern / Area of Concern

Description of Information or Topic(s) Requested (In your own words)

Data subject declaration

I request that the School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School.

I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent)

…………………………………………

Name of "Data Subject" (or Subject's Parent)

(PRINTED)…………………………………………..

Dated …………………………………………..