St Katherine's School

Data Protection and Security Policy

Policy Number SKP C 006

Next Review: **April 2017**

Signed : _____ **Dated :** _____

Headteacher

Signed: _____ **Dated :** _____

Chair of Governors

1 Introduction

1.1 The purpose of this document is to ensure that all users and keepers of data (staff, PGCE students and temporary staff) of St Katherine's School are aware of the rules regarding personal data and the Freedom of Information Act 2000 (FOIA).

1.2 It is the responsibility of all users and keepers of data in St Katherine's School to be aware of and follow all St Katherine's School Data policies and guidelines and to seek advice in case of doubt.

1.3 This policy may be updated or supplemented by specific standards or procedures to reflect further developments in technology or legislation or other relevant changes.

1.4 The following terminology will be used throughout this document:

- Personal data – data relating to any identifiable living individual; this can take the form of electronic or manual records as well as photographic and CCTV images.
- Sensitive personal data – personal data relating to an identifiable individual's mental or physical health, race/ethnic origin, religious or political beliefs, sexual orientation or trade union membership.
- Data subject – an individual to whom any personal data relates.
- Data controller – any organisation that is responsible for processing personal data.
- Data processor – any organisation that processes personal data on behalf of a data controller.
  (St. Katherine's School is registered both as a Data controller and a Data Processor.)

The definitions and material quoted in this document have been taken from *The Guide to Data Protection* issued by the Information Commissioner's Office.

Specific guidance on the use of photographs in school can be obtained from the Information Commissioner's Office website:
http://ico.org.uk/for_the_public/topic_specific_guides/schools/photos

Specific guidance on the use of Biometric Technology in school can be obtained from the Information Commissioner's Office web site:
http://ico.org.uk/for_the_public/topic_specific_guides/schools/fingerprinting

2 Data protection

2.1 Definitions

Schools hold information on pupils and in doing so must follow the requirements of the 1998 DPA. This means that data held about pupils must only be used for specific purposes that are allowed by the Act. The rules regarding personal data also apply to employees, whether they are teaching or non-teaching staff.

Schools are 'data controllers' under the Act in that they process 'personal data' in which people can be identified individually. When data is obtained from data subjects the data controller must ensure, so far as is practicable, that the data subjects have, or are provided with, or have readily available to them, the following information, referred to as the 'fair processing information':

- Details of the data that they hold on them
- The purposes for which they hold the data
- Any third parties to whom the information may be passed.

The DPA updated the rules and regulations on the protection of the individual and extended the principles to apply to all personal data that is processed. The DPA covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of data and there are eight principles that must be adhered to as well as a number of conditions that apply. The DPA has been extended to apply to paper files as well as electronic data, so the principles now apply to records and notes that are kept, for example, in teachers' mark books.

The Data Protection Principles state:

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

(a) at least one of the conditions in Schedule 2 of the DPA is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 of the DPA is also met.

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 those 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 for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under the Act.

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

8. 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.

Each school that processes data must notify the Information Commissioner annually of that fact. St. Katherine's Schools Registration number is Z5700110 and Registration expires on 18 October each year.

2.2 Personal data should be processed fairly and lawfully

The DPA sets out a 'fair processing' code. This requires data controllers to inform subjects about the purposes for which their personal data will be processed. This information should be provided at the time the personal data is obtained from the data subject, and should be comprehensive and transparent.

Problems may arise in providing this information for young children. The guidance is that as soon as children are able to understand their rights under the Act, they should exercise these rights on their own. The Information Commissioner's guidance is that children by the age of 12 have sufficient understanding to make their own decisions, but there may be exceptions to this view. This means that it may be acceptable to ask students in Year 8 and above to give permission for the storing and processing of data (which includes photographs) but it is recommended that parental permission is sought for all students below Year 12.

Wherever possible, written consent should be obtained from the parent or student at the time that data is collected. See Appendix 1 for an example.

2.3 Data security

Users must only access data held on St Katherine's School's computer systems if they have been properly authorised to do so. Shared data areas on the server exist where staff is required to share files, carry out work or contribute to project collaborations. If there is any doubt about access rights to any data area, please contact ICT Support and/or the project coordinator responsible for the data to be accessed. It is school policy for users to store data on a network drive where it is regularly backed up.

Staff with Laptops must remember that data from their network 'home' drive is synchronised with their laptop. If the Laptop is stolen, this could lead to data falling into unauthorised hands. Staff must ensure that their Laptop access is protected by a strong password (see Password Policy – Appendix 2) and must store only data which is needed at home in this area. When reporting a laptop theft, the member of staff must provide a list of all personal data or sensitive personal data held.

Under no circumstances should any user disclose personal or other confidential information held on computer to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computers' Misuse Act 1990. In particular, no person may use the school SIMS system or any other central database, to extract data via a report or by hand, using electronic means, photographic means or paper and then use the data or allow it to be used away from the school premises without the express consent of the Headteacher. This applies even if the person is authorised to view the data in school.

Staff should note that all data and correspondence, including e-mail messages, held by St Katherine's School (including that on school laptops) may be provided to a data subject, internal or external, in the event of a subject access request.

2.4 Email
St. Katherine's School issues email addresses to all students and to all staff. Student and staff addresses are based on their network user names but are kept separately. Email messages cannot be considered to be private, secure or temporary.

The email user must be consulted before their email address is passed on to anyone else.
Please refer to policy SKP C005 ICT Acceptable Use Policy for more details.

2.5 School Website (www.st-katherines.n-somerset.sch.uk)
St Katherine's School has a web site which is used to pass on information to parents and others in the wider community. It is constructed under the following guidance:

• A school website should take care to protect the identity of pupils: where a child's image appears, the name should not, and vice versa.

• Parental permission should be obtained before using images of pupils on the website.
If a school collects personal data in any form via its website this may be subject to data protection legislation; a clear and detailed privacy statement should be displayed prominently on the site stating how the information will be used. Schools should also take care to protect intellectual property on their site, and should not provide any information which could be in breach of copyright law.

2.6 Cashless Catering System

Biometric Registration
Each individuals finger and thumb prints are unique. The Biometric cashless system will store only a section of the print as a unique number and not as an image. Each child will have that unique number stored on a central server. This is done by scanning the finger or thumb with a non-invasive electronic scanner, which passes light over the finger or thumb. The same scanner will be installed at the tills where they 'pay' for their food.

A print will be stored numerically, as a set of between 20 and 50 reference points, unique to the individuals print. Each reference point comprises of three numbers which are the X and Y co-ordinates and an angle of curve. The system does not store the image of the finger scanned. The stored co-ordinates are only of use in matching part of the individuals print and cannot be used for the purpose of reconstructing a print.

The numbers will be held in a secure SQL database on the server. Access to this database is given only by the school and then only to those who are required to administer the system.

Data Handling
Certain data will be held on the system to enable accurate operation. This will include a child's name, class, photo, account balance and meal entitlement. This data will be handled under the guidelines of the DPA and only used by parties directly associated with the school. Access to this information is controlled strictly by the school only.

2.7 Freedom of Information Act 2000
St. Katherine's School is subject to the provisions of the FOIA which provides for the general right of access to information held by public authorities and as such has to have a publication scheme. The definition guidance for schools in England gives examples of the kinds of information that is expected to be provided in order to meet our commitments under the FOIA model publication scheme. The definition guidance document can be found at:

https://ico.org.uk/for_organisations/sector_guides/~/media/documents/library/Freedom_of_Information/Detailed_specialist_guides/definition-document-schools-in-england.pdf

For a request to be valid under the Freedom of Information Act it must be in writing, but requesters do not have to mention the Act or direct their request to a designated member of staff.

Under the Act, most public authorities may take up to 20 working days to respond, counting the first working day after the request is received as the first day. For schools, the standard time limit is 20 school days, or 60 working days if this is shorter.

The ICO guidance should be read in conjunction with the separate Department for Education (DfE) advice issued under The School Information (England)(Amendment) Regulations 2012, which details what schools should publish online. This guidance can be found at: https://www.gov.uk/what-maintained-schools-must-publish-online

The model publication scheme can be found at Appendix 3.

While St Katherine's School is in the process of meeting the requirements of the Act, staff and governors should be aware that the Act also extends Subject Access Request (SAR) rights available under the DPA to include all types of information held, whether personal or non-personal.

SAR are handled by reference to the Subject Access Code of Practice which also covers special consideration given to the release of information related to child protection. Ac opy of the guidance can be found at:
https://ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf

2.7.1 Pupil information
A pupil, or someone acting on their behalf, may make a SAR in respect of personal data held about the pupil by the school.

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

- The pupil's right of subject access under the DPA; and
- The parent's right of access to their child's 'educational record'

It is important to understand what is meant by a pupil's 'educational record'. This is because there is an overlap between the two rights mentioned above, and also because 'educational record' is relevant when deciding the fee the school may charge for responding to a SAR. Broadly speaking, however, the expression has a wide meaning and includes most information about current and past pupils that is processed by or on behalf of the school.

However, information kept by a teacher solely for their own use does not form part of the educational record. It is likely that most of the personal information the school holds about a particular pupil will form part of the pupil's educational record. However, it is possible that some of the information could fall outside the educational record; e.g., information about the pupil provided by the parent of another child is not part of the educational record.

Unlike the distinct right of access to the educational record, the right to make a SAR is the pupil's right. Parents are only entitled to access information about their child by making a SAR if the child is unable to act on their own behalf or has given their consent. If it is not clear whether a requester has parental responsibility for the child or is acting on their behalf, the school should clarify this before responding to the SAR.

2.7.2 Exemptions
In deciding what information to supply in response to a SAR, the school needs to have regard to the general principles about exemptions from subject access. Examples of information which (depending on the circumstances) it might be appropriate to withhold include:

• Information that might cause serious harm to the physical or mental health of the pupil or another individual;
• Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests;
• Information contained in adoption and parental order records; and
• Certain information given to a court in proceedings concerning the child.

2.7.3 Charges
If a SAR is made for information containing, in whole or in part, a pupil's 'educational record', a response must be provided within 15 school days. The maximum amount you may charge for dealing with the request depends on the number of pages of information to be supplied.

The following table shows the maximum fees:

Number of pages of information supplied	Maximum fee
1-19	£1
20-29	£2
30-39	£3
40-49	£4
50-59	£5
60-59	£6
70-79	£7
80-89	£8
90-99	£9
100-149	£10
150-199	£15
200-249	£20
250-299	£25
300-349	£30
350-399	£35
400-449	£40
450-499	£45
500+	£50

Special cases:
If the SAR does not relate to any information that forms part of the educational record, then the usual 40-day time limit for responding applies. The maximum fee for dealing with the request is £10.

2.7.4 Information about examinations
Special rules apply to SARs relating to information about the outcome of academic, professional or other examinations.

These rules, which apply to requests for examination scripts, marks or markers' comments, are designed to prevent the right of subject access being used as a means of circumventing an examination body's processes for announcing results.

Information comprising the answers given by a candidate during an examination are exempt from the right of subject access. So a SAR cannot be used to obtain a copy of an individual's examination script.

Although this exemption does not extend to an examiner's comments on a candidate's performance in an examination (whether those comments are marked on the examination script or recorded on a separate marking sheet), or to details of the marks awarded, there is a special rule governing the time limit for responding to a SAR for such information in cases where the SAR is made before the results are announced. In such cases, a response must be provided within the earlier of:

- Five months of the date of the request; and
- 40 days of the date on which the results are announced.

Where a SAR is made for an individual's examination marks, a response may only be refused (or delayed) for reasons permitted by the DPA. So it would not be appropriate to refuse to provide details of examination marks in response to a SAR because the requester had failed to pay their tuition fees. Clearly, though, providing information about examination results is not the same as conferring a qualification.

2.8 Photography

St. Katherine's School uses school-provided cameras to take photographs and videos of students and staff. These media files are defined as personal information by the DPA and must be treated as such. Consent is sought from parents and carers through the parent information pack which is sent out before a pupil joins St. Katherine's. If a group is to be photographed or recorded the consent list must be checked. The processing and storage of images or videos must be in line with the rest of this policy and the DPA.

3 Passing on Information

3.1 Introduction

Schools hold information about children and adults and they process it in a number of ways to improve the quality and standard of their provision. Information is passed electronically from schools to LEAs (pupil transfer data, for example) and examination boards. Schools and LEAs pass information to a number of statutory bodies (such as QCA and Connexions), and to contractors who provide other services (content providers, such as CATS or SAM Learning). Additionally, the Children and Young People's Unit (CYPU) requires local authorities, where necessary, to share information with other local government partners to identify children and young people in danger of social exclusion.

St. Katherine's School will attempt to ensure that measures are in place for the safety and integrity of the data which is passed on and that it will not be used for any purpose other than that for which it was collected and that it will be destroyed when it is no longer needed.

3.2 Disposal

All St. Katherine's desktop PCs, laptops and servers will be disposed of securely with the data being destroyed in accordance with DOD5220.22M standards.

It is the responsibility of the user to ensure that copies of any personal files are obtained before the laptop is handed back for disposal or reuse.

3.3 Staff from External Agencies

Staff from external agencies, such as employees of North Somerset Council or Connexions, may be given access to the school network and to appropriate data held in it. Such persons must be identified (preferably in writing) in advance and must carry and wear an appropriate employee identification badge.

Any such person will be required to sign a copy of the Acceptable Use Policy and abide by the school policies.

Access will only be given to those areas which are appropriate to the work of that person in school and will be controlled by network and application user names and passwords. The person will be required to process this data only in accordance with their own terms of employment and will be forbidden from removing data from the system without authorisation from their employer and the Head Teacher of the school.

4 The School's Legal Responsibilities

4.1 Requirements

St. Katherine's School conforms to the requirements of the DPA and the FOIA.

4.2 Storage of Data

The fifth principle of the DPA states that "Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes."

The guidance suggests that:

- Finance Data should be kept for 6 years or as laid down by Local Authority Financial Regulations.
- Pupil and Staff Data should be kept for 7 years, after which a school might not be required to provide exam results or references.
- In practice, core data archived by the SIMS system may be kept for longer than this, depending on the recommended configuration of the system.

All paper documentation stored/archived at the school is securely destroyed by a recognised data handling contractor as per the schedule contained in the *Records Management for Schools Toolkit* provided by the Information and Records Management Society. A copy of the toolkit is available at: http://www.irms.org.uk/resources/information-guides/199-rm-toolkit-for-school

4.3 Updates to this Policy

In the light of changes in the business, technology, legislation or relevant standards it may be necessary to update this policy from time to time. Notification to all staff will be made when updates are available.

4.4 Disciplinary and related action

St Katherine's School wishes to promote the highest standards in relation to good practice and security in the use of data. Consequently it expects and supports the integrity of its staff. In exceptional circumstances, where there are reasonable grounds to suspect that an employee has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

Appendix 1

Example School Trip to the Isle of Wight

- Data collection for the school trip begins as soon as students (and staff) express an interest in going on the trip.
- They will take home a letter with details of the trip. This letter should explain how bookings and payments are to be recorded.
- Once they have been accepted, they will start to pay in money and the school Finance database will be used. It is also likely that the leader will keep written or electronic records. The Finance database is stored on the school network, but the leader's record may be a simple written list. This list must be kept secure. It would be a breach of the Act to pass on names, for example to a hotel, if this was not mentioned in the letter.
- The school SIMS database holds essential data about student's medical conditions, as provided by parents when the child enters the school or later. The leader may consult the database, but may not pass on any information there, for example to a hotel or coach company, without the permission of the data subject.
- The leader will organise a parents' meeting about the trip and may hand out forms asking for contact information and/or medical information. The form should state clearly where this data will be stored and what will be done with the forms once the trip is over.
- The leader will also ask for permission to take photographs of the students on the trip and will state how those photographs may be used. If video filming is planned, then this must be included in the permission slip.
- Before departure, the leader may photocopy these forms to give to other staff who will accompany the students, or may extract relevant data and print it as a separate document. These copies or extracts must be treated like the original information. In particular, they should not be further copied. If a copy is left in school, it must be kept secure.
- On the day of departure the leaders will ensure that the information they hold is kept secure. For overseas travel, this information would be kept in hand luggage and not "checked in".
- On return, the leader and other staff will securely dispose of the information.
- If permission was given, photographs may be collected and video footage edited. The photos or video may be stored on the school network and may be used in a presentation, as long as permission was given for this.
- Photos may be used on the web site, or school newsletter, if permission was given, but names must NOT be given.

Appendix 2

Password Policy

Access to the School Network and to data stored on it is controlled by usernames and passwords. Special database programs, such as the SIMS system, have separate access controls in addition to this.

User names and passwords must never be communicated to any other person, nor should any person log in to the network for another person. This could result in unauthorised access to information.

Network passwords must:

- be at least 6 characters in length.
- contain a mixture or letters and numbers.
- ideally contain at least one capital letter (passwords are case sensitive).

The network will force the user to choose a new password at least twice a year. Users cannot re-use the last 24 passwords.

It is not good practice to use the same password for all applications, though it can be sensible to have a small number of passwords in use at any time.

Passwords must never be written down or shared.

Appendix 3

Model Publication Scheme
Freedom of Information Act

This model publication scheme has been prepared and approved by the Information Commissioner. It may be adopted without modification by any public authority without further approval and will be valid until further notice.

This publication scheme commits an authority to make information available to the public as part of its normal business activities. The information covered is included in the classes of information mentioned below, where this information is held by the authority. Additional assistance is provided to the definition of these classes in sector specific guidance manuals issued by the Information Commissioner.

The scheme commits an authority:

- To proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by the authority and falls within the classifications below.

- To specify the information which is held by the authority and falls within the classifications below.

- To proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within this scheme.

- To produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public.

- To review and update on a regular basis the information the authority makes available under this scheme.

- To produce a schedule of any fees charged for access to information which is made proactively available.

- To make this publication scheme available to the public.

- To publish any dataset held by the authority that has been requested, and any updated versions it holds, unless the authority is satisfied that it is not appropriate to do so; to publish the dataset, where reasonably practicable, in an electronic form that is capable of re-use; and, if any information in the dataset is a relevant copyright work and the public authority is the only owner, to make the information available for re-use under a specified licence. The term ‘dataset’ is defined in section 11(5) of the Freedom of Information Act. The terms ‘relevant copyright work’ and ‘specified licence’ are defined in section 19(8) of that Act.

Classes of information:

Who we are and what we do
Organisational information, locations and contacts, constitutional and legal governance.

What we spend and how we spend it
Financial information relating to projected and actual income and expenditure, tendering, procurement and contracts.

What our priorities are and how we are doing
Strategy and performance information, plans, assessments, inspections and reviews.

How we make decisions
Policy proposals and decisions. Decision making processes, internal criteria and procedures, consultations.

Our policies and procedures
Current written protocols for delivering our functions and responsibilities.

Lists and registers
Information held in registers required by law and other lists and registers relating to the functions of the authority.

The services we offer
Advice and guidance, booklets and leaflets, transactions and media releases. A description of the services offered.

The classes of information will not generally include:

- Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.
- Information in draft form.
- Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons.
- The method by which information published under this scheme will be made available

The authority will indicate clearly to the public what information is covered by this scheme and how it can be obtained.

Where it is within the capability of a public authority, information will be provided on a website.

Where it is impracticable to make information available on a website or when an individual does not wish to access the the website, a public authority will indicate how information can be obtained by other means and provide it by those means.

In exceptional circumstances some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.

Information will be provided in the language in which it is held or in such other language that is legally required. Where an authority is legally required to translate any information, it will do so.

Obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats will be adhered to when providing information in accordance with this scheme.

Charges which may be made for information published under this scheme:

The purpose of this scheme is to make the maximum amount of information readily available at minimum inconvenience and cost to the public. Charges made by the authority for routinely published material will be justified and transparent and kept to a minimum.

Material which is published and accessed on a website will be provided free of charge.

Charges may be made for information subject to a charging regime specified by Parliament.

Charges may be made for actual disbursements incurred such as:

- photocopying
- postage and packaging
- the costs directly incurred as a result of viewing information

Charges may also be made for information provided under this scheme where they are legally authorised, they are in all the circumstances, including the general principles of the right of access to information held by public authorities, justified and are in accordance with a published schedule or schedules of fees which is readily available to the public.

Charges may also be made for making datasets (or parts of datasets) that are relevant copyright works available for re-use. These charges will be in accordance with either regulations made under section 11B of the Freedom of Information Act or other enactments.

If a charge is to be made, confirmation of the payment due will be given before the information is provided. Payment may be requested prior to provision of the information.

Written requests:

Information held by a public authority that is not published under this scheme can be requested in writing, when its provision will be considered in accordance with the provisions of the Freedom of Information Act.