"I have come in order that you might have life – life in all its fullness."
John 10:10

Data Protection and Information Security Policy

Incorporating reference to the General Data Protection Regulation (GDPR)

Policy accepted by FGB on:	8/2/2018
Next review:	Spring 2019
Signed (Chair of Governors):	
Statutory policy: Yes/No **On school website:** Yes/No	

Contents

Data Protection and Information Security:
Key Information

Role	Person responsible
Data Protection Officer (eLIM)	**Ian Gover**
Data Protection Lead (School)	**Rupert Kaye (Headteacher)**
System Manager (School)	**Rupert Kaye (Headteacher)**
Nominated Officer (School)	**Sara Lodge (School Business Manager)**
Data Protection Champion (School)	**Jessica Slater (Governor)**

DATA PROTECTION AND INFORMATION SECURITY POLICY

(This policy is based on Somerset County Council's *e-Learning and Information Management* (eLIM) model policy and conforms to the model scheme for schools approved by the Information Commissioner. This policy should be read in conjunction with both Christ Church's Freedom of Information Policy and Freedom of Information Publication Scheme.)

Part One: Data Protection (eLIM model policy 2017–18, incorporating the General Data Protection Regulation (GDPR))

1.1 Introduction to data protection

Christ Church needs to keep information about our pupils, staff and other users to allow us to follow our legal and statutory duties and to provide other services.

Christ Church will comply with the data protection principles which are set out in the General Data Protection Regulation and other laws.

1.2 The Data Controller and the designated Data Controllers

The school, as a body, is the Data Controller.

The school has identified its designated Data Protection Officer (DPO) (see page 3, above), who will deal with matters detailed in section 1.10 (below).

Other day-to-day matters will be dealt with by the System Manager/Data Protection Lead (the Headteacher), Deputy Headteacher and the School Business Manager (the Nominated Officer).

1.3 Responsibilities of the school

The school is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, parents and governors. This implies that:

a) all systems that involve personal data or confidential information will be examined to see that they meet the requirements of the General Data Protection Regulation;
b) the school will inform all users about their rights regarding data protection;
c) the school will provide training to ensure that staff know their responsibilities;
d) the school will monitor its data protection and information security processes on a regular basis, changing practices if necessary.

1.4 Responsibilities of Staff

All staff are responsible for checking that any information that they provide to the school is accurate and up to date. All staff are also responsible for ensuring that any

personal data they use in the process of completing their role:

a) is not in the view of others when being used;
b) is kept securely in a locked filing cabinet or drawer when not being used;
c) be password protected both on a local hard drive and on a network drive that is regularly backed up;
d) if kept on a laptop, USB memory sticks or other removable storage media, is password protected and encrypted. The device must be kept in a locked filing cabinet, drawer or safe when not in use. The data held on these devices must be backed up regularly;
e) is not disclosed either orally or in writing or via web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure or transgression of the above statements will usually be a disciplinary matter.

1.5 Responsibilities of parents/guardians

The school will inform the parents/guardians of the importance of and how to make any changes or deletions to personal data. This includes an annual data collection sheet with the return of this document being recorded.

Other permissions will also be sought regarding matters of non-statutory use of personal data such as the use of images and use of names in publicity materials on induction, annually or when required. The returns to these permissions will be recorded and exemptions communicated to staff.

1.6 Rights to access information

All people having personal data stored by the school have the following rights:

a) To obtain from the school confirmation as to whether personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
    i) the purposes of the processing;
    ii) the categories of personal data concerned;
    iii) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular, recipients in third countries or international organisations;
    iv) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
    v) the existence of the right to request from the school rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
    vi) the right to lodge a complaint with a supervisory authority;
    vii) where the personal data are not collected from the data subject, any available information as to their source;

viii) the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

b) Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

c) To have a copy of the personal data undergoing processing. For any further copies requested by the data subject, the school may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

d) Where the data subject obtains a copy referred to in paragraph (c), this shall not adversely affect the rights and freedoms of others.

The school will place on its website Privacy Notices regarding the personal data held about them and the reasons for which it is processed.

All staff, parents and other users have a right to ask to view personal data being kept about them or their child, called a 'subject access request'. Any person who wishes to exercise this right should make a request in writing and submit it to the Headteacher. The process for dealing with these requests is outlined in section 1.11 (below).

The school aims to comply with requests for access to personal information as quickly as possible and in compliance with advice from the Information Commissioner's Office (ICO) and other professional agencies. There may be an administration charge, which will be stated once the enquiry is made.

There is a separate policy for the processing of Freedom of Information requests.

1.7 Data breaches

If there is a data breach, the school will inform the DPO, who will then advise on any actions. Any data breaches will be recorded, comprising the facts relating to the personal data breach, its effects and the remedial action taken. If there are risks to the individual, the school will communicate the breach to the data subject.

In the case of a personal data breach where there is a high risk to the rights and freedoms of the data subject, the DPO shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority.

1.8 Reporting policy incidents

Any member of staff, parent or other individual who considers that the policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the Headteacher, in the first instance. Alternatively, they could contact the DPO directly.

1.9 Monitoring and evaluation

This policy will be monitored and reviewed in line with the school's policy review schedule.

1.10 Role of Data Processing Officer

According to Article 37(5), the DPO, who can be a staff member or contractor, shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices, and the ability to fulfil the tasks referred to in Article 39. These are:

- to inform and advise the controller or the processor and the employees who are processing personal data of their obligations pursuant to this Regulation;
- to monitor compliance with this Regulation, including the assignment of responsibilities, awareness-raising and training of staff involved in the processing operations, and the related audits;
- to provide advice where requested about the data protection impact assessment and monitor its performance pursuant to Article 35;
- to cooperate with the supervisory authority (the ICO in the UK);
- to act as the contact point for the supervisory authority on issues related to the processing of personal data.

1.11 Process for dealing with a subject access request or request for change or deletion of data

On receiving a subject access request or request for change or deletion of data, the school will:

- inform the Data Protection Lead in the school (the Headteacher);
- record the details of the request, updating this record where necessary;
- reply to the requestor, informing receipt of the request and asking for clarity if there is confusion about which data is required;
- make contact with the DPO if clarity on the request is needed or procedure is needed;
- identify the people responsible for gathering the necessary data;
- gather the data indicating a deadline;
- examine the data for redactions, making sure there is no "bleeding" of data;
- ask the requestor for an address and time for delivery.

The whole process should take no longer than 30 days, which can be extended by a further two months where the request is complex or where there are numerous requests.

Part Two: Information Security

2.1 Introduction to information security

The purpose for controlling access to data is to ensure that only authorised personnel are able to access information that is relevant to the tasks for which they are responsible. It prevents unauthorised access to information, which could result in accidental or deliberate corruption of the data and which might contravene the confidentiality part of the Data Protection Act 1998 (DPA).

One person, the Headteacher (System Manager), is responsible for the overall control of all systems, with the Deputy Head covering for absence. Ongoing day-to-day responsibility for the controlled access to all data in the school in accordance with the DPA has been delegated to the School Business Manager (the Nominated Officer), who will ensure that all staff are aware of their responsibilities/obligations at all times.

The school and Governing Body register annually under the DPA. At Christ Church C of E First School, the System Manager (i.e. the Headteacher) has delegated ongoing day-to-day responsibility for the controlled access to all data in the school in accordance with the DPA to the School Business Manager. The School Business Manager, as Nominated Officer, shall further ensure that information relating to personnel is:

- obtained and processed fairly and lawfully;
- held only for specified lawful purposes;
- adequate and relevant but not excessive for those purposes;
- accurate and up to date;
- available to those people referred to;
- kept securely.

Information should not be kept longer than necessary and neither used nor disclosed other than in accordance with the above purposes.

Any new use of personal information is notified to the DPO at County Hall. Offences against the DPA are criminal, and individuals will be held personally responsible.

Individual members of staff can be personally liable in law under the terms of the DPA and related legislation. 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 policy will be treated as a disciplinary matter, and serious breaches could lead to dismissal.

2.2 Fair obtaining and processing of data

Christ Church C of E First 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 is 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.

Definitions:

- **"processing"** means obtaining, recording or holding the information or data, or carrying out any or a set of operations on the information or data.
- **"data subject"** means an individual who is the subject of personal data or the person to whom the information relates.
- **"personal data"** means data which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so also are names and photographs, if published in the press, on the Internet or social media.
- **"parent"** has the meaning given in the Education Act 1996, and includes any person having parental responsibility or care of a child.

2.3 Registered purposes

The Data Protection Register 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 School Business Manager, who, as Nominated Officer, deals 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.

2.4 Data integrity

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

A. *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. 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". 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 judgment. 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.

B. ***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. *(Details should be added on how and when records are checked for irrelevant data and who has the say on what must be deleted.)*

C. ***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 School Business Manager/office administrator to ensure that obsolete data is properly erased.

2.5 <u>Subject access</u>

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 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.

2.6 <u>Processing subject access requests</u>

Requests for access must be made in writing.

Pupils, parents or staff may ask for a Data Subject Access Form (Appendix B), available from the school office. Completed forms should be submitted to the School

Business Manager (the Nominated Officer). 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 (e.g. 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) (England) Regulations.

2.7 Authorised disclosures

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

These circumstances are strictly limited to the following:

- 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, e.g. 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 LA are IT liaison/data processing officers, for example in the LA, and 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 needs 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 which suggests that they are, or have been, either the subject of, or at risk of, child abuse.

Definitions:

- 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.

2.8 Data and computer security

Christ Church C of E First School undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed):

A. Physical security

Appropriate building security measures are in place, such as alarms, window bars, and deadlocks.

Only authorised persons, e.g. school staff (paid or unpaid) and governors are allowed in the school office. Children may only enter if accompanied by an authorised person.

All visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

B. 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.

C. Procedural security

In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their data protection obligations and their knowledge updated as necessary.

Computers should not be left unattended with information displayed on the screen, or be easily accessible by any unauthorised users. Where possible, computer screens are locked (by password/locking the workstation), or if this is not possible, the computer is closed down whilst it is left unattended.

Access to software is restricted according to the level of access required for an individual to carry out their job to an expected level. These access rights are reviewed regularly by the System Manager (Headteacher) and Nominated Officer (School Business Manager).

Only licensed software, authorised by Somerset County Council's IT Department, should be installed onto the school's network, which is protected through a virus guard so that any files received from outside sources can be virus checked before being opened.

i) *Passwords*

Individuals are responsible for the accuracy of information which is kept secure from unauthorised persons. Passwords must:

- not be told to anyone else;
- never be typed in when someone is watching;

- be changed regularly, e.g. every three months, or as soon as someone else finds out about it;
- be difficult for someone else to guess, i.e. avoid using names etc.;
- a mixture of alphabetic and numeric characters.

Full access to SIMS FMS is restricted to the school's System Manager (Headteacher) and Nominated Officer (School Business Manager) only.

ii) *Servers*

With the development of ICT software and hardware, the server is not used as an everyday machine. Therefore, it is stored in a discreet place within the office and should never be turned off, to ensure backup procedures are not compromised.

ii) *Backup*

Backup copies of all data held on the school network (P:Drive) are made automatically overnight. They are held online and are monitored daily by Futurform. Data servers are held in the UK. Data is backed up on servers in London and Maidenhead.

iii) *Virus protection*

Current versions of antivirus software are installed on the network's server to safeguard it against viruses and to avoid any corruption of data. Using only authorised software will contribute to this protection.

iv) *Computer printouts*

Each month, the Finance Officer downloads and prints details of expenditure recorded on the County Council's Accounting System relating to the school's budget. These printouts are used in the SIMS FMS reconciliation process to ensure that the school's financial records match those recorded by Somerset County Council. They are stored carefully in a lockable cabinet, as they contain personal information relating to staff employed at the school, for three years plus the current year. Computer printouts, as well as source documents, are shredded before disposal.

2.9 Responsible Internet use

Rules for using the Internet are set out in the following school policies:

- Acceptable Use Policy
- Social Media and Social Networking Policy

2.10 Freedom of information

Christ Church C of E First School is registered with the Information Commissioner and has a separate Freedom of Information Policy.

APPENDIX A: INFORMATION COMMITMENT

Your information. Our commitment.

Christ Church C of E First School holds a great deal of information, much of which is confidential. This may be information about:

- our pupils;
- our pupils' parents or guardians;
- our governors;
- our staff.

We will comply with the provisions of the Data Protection Act 1998 and any subsequent legislation relating to information handling and privacy. Christ Church has an Information Security Policy, which relates to best practice in terms of both data security and the ethical use of that data.

If we hold information about you, we wish to assure you that we are processing the information fairly and lawfully, and that we will inform you of the purposes for which we require the information when you supply it to us. In particular:

When we collect information

- We will only collect information that is necessary for what we do.
- We will be fair in the way we collect information about you.
- We will tell you who we are and what we intend to do with the information about you.
- Where practicable, we will collect information which relates to you directly from you.
- If we collect information about you from someone else, we will, wherever possible, make sure you know that we have done this.

When we use and disclose information about you

- We will only use or disclose your information for legitimate purposes about which you have been told, unless we are required to do otherwise for legal reasons.

Information quality

- We will ensure that information about you is accurate and up to date when we collect or use it. You can help us to achieve this by keeping us informed of any changes to the information we hold about you.

Information security

- We will keep information about you secure.
- We will protect your information against unauthorised use, damage, loss and theft.

Retention

- We will hold information about you for as long as is necessary but, subject to any statutory retention periods, we will ensure that the information is disposed of in a secure and proper manner when it is no longer needed.

Openness

- We will be open with you about what kinds of information we hold and what we do with it.

Access and correction

- Wherever possible, we will let you see the information we hold about you (should you wish) and correct it if it is wrong.

If you need a more detailed explanation of any of the commitments made in this statement, please contact the school.

Rupert Kaye Headteacher (System Manager & Data Protection Lead)	Sara Lodge School Business Manager (Nominated Officer)

APPENDIX B: DATA SUBJECT ACCESS FORM

DATA REQUEST

I request that the school search its records based on the information supplied below 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 below relating to me (or my child/children) being processed/held by the school.

Enquirer's Surname ……

Enquirer's Forename(s) ……..……..

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

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

If YES, what is/are the name(s) of the 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)

……..…….

……..…….

Additional information

……..…….

……..…….

Please despatch reply to: *(if different from enquirer's details as stated on this form)*

Name ……..…….

Address ……..…….

……..…… Postcode ……..

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/held 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 that I have authorised to receive such information).

Signature of Data Subject (or Subject's Parent) …….

Name of Data Subject (or Subject's Parent) …… (PLEASE PRINT)

Date ……..