Policy Document:	DATA PROTECTION POLICY
School's Lead Member of Staff:	HEADTEACHER
Lead Governors (monitoring):	FULL GOVERNORS
Revision Date:	November 2025
Document Version:	1.2 (Reviewed November 2025 with minor changes)
Governor Committee:	FULL GOVERNORS
Committee Approval Date:	14 May 2019
Full Governors Ratification Date:	14 May 2019
Review Frequency:	2 YEAR
Date of next review:	November 2027
Publication Date:	November 2025
Purpose:	To ensure that the Headteacher and Governing Body act in accordance with the law on Data Protection.

Chair of Governing Body Signature:

Data Protection Policy

Contents

1. Executive Summary

2 Policy statement

3 About this policy

4 Definition of data protection terms

5 Data protection Coordinator

6 Data protection principles

7 Fair and lawful processing

8 Processing for limited purposes

9 Notifying data subjects

10 Adequate relevant and non-excessive

11 Accurate data

12 Timely processing

13 Processing in line with data subject's rights

14 Data security

15 Data protection impact assessments

16 Disclosure and sharing of personal information

17 Data processors

18 Images and videos

19 Changes to this policy

ANNEX Definition of terms

1. EXECUTIVE SUMMARY

As a School we are committed to ensuring that we follow all statutory and best practice guidelines in relation to data protection and security.

This policy sets out how data is secured and how we monitor processes and address data breaches in accordance with the latest legislation and guidance.

Key messages:

➢ As a 'data controller' CFS has legal responsibilities to ensure personal data is only gathered as necessary, is securely stored and is only shared in accordance with the latest legislation and guidance (Section 2)

➢ This Policy sets out legal definitions (Sections 3 and 6) and how CFS organises and monitors Data Protection (Section 5) to ensure that all data is "fair and lawful" (Section 7), timely and accurate (Section 8) and secure (Section 14)

➢ The rights of those on whom we collect and store personal information (Data Subjects) are explained (Section 2 and 13), including how we will notify/disclose to them (Section 9 and 16) and how we will seek their consent (Section 7)

➢ The Policy also sets out the various key roles and responsibilities (Section 5).

2. Policy statement

Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities as a school we will collect, store and **process personal data** about our pupils, **workforce**, parents and others. This makes us a **data controller** in relation to that **personal data**.

We are committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.

The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.

All members of our **workforce** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

3. About this policy

The types of **personal data** that we may be required to handle include information about pupils, parents, our **workforce**, and others that we deal with. The **personal data** which we hold is subject to certain legal safeguards specified in the General Data Protection Regulation ('**GDPR**'), the [Data Protection Act 2018], and other regulations (together '**Data Protection Legislation**').

This policy and any other documents referred to in it set out the basis on which we will **process** any **personal data** we collect from **data subjects**, or that is provided to us by **data subjects** or other sources.

This policy does not form part of any employee's contract of employment and may be amended at any time.

This policy sets out rules on data protection and the legal conditions that must be satisfied when we process **personal data**.

4. Definition of data protection terms

All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in the Annex to this policy.

5. ROLES AND RESPONSIBILITIES

- **Governing body**

○ Approve the policy, ensuring it reflects statutory guidance (e.g. UK GDPR).

○ Hold senior leaders to account for the effective implementation of the policy in day-to-day practice.

○ Assure itself that there is a culture in school of effective Data Protection and safe, lawful and timely data gathering, storage and sharing.

○ Assure themselves and external bodies that the policy is clear and well-understood by all staff, implemented consistently across the school and reviewed regularly in response to legislative updates or safeguarding incidents.

- **Head Teacher**

○ Provide leadership and oversight of this Data Protection Policy and its implementation, ensuring that data is shared appropriately and legally with external bodies and partners.

○ Provide assurance to the Governors the school has a clear, lawful and up-to-date Data Protection Policy, robust processes and positive culture in regard to Data Protection.

- **IT Manager/IT Admin**

○ Oversee the technical infrastructure that supports safe, lawful and secure Data Protection internally and with external agencies and other third parties.

- **Business Manager**

○ Oversee and monitor the implementation of the policy within the school's administration function.

○ Review and report to Senior Leaders/Governors on a regular basis, routinely and on any event or change.

○ Review functionality of DPC and liaise with any external bodies as necessary to ensure compliance and best practice.

- **Heads of School/Departments**

○ Cascade training down to staff within their teams, ensuring staff understand and implement this policy

○ Report problems or concerns back to the Headteacher, Data Protection Coordinator or Business Manager.

- **Data Protection Officer and Coordinator**

As a small independent school, we do not have an internal Data Protection Officer (DPO) - this role is outsourced to Judicium Education. Our data, day to day responsibilities are coordinated by our

Data Protection Coordinator (DPC). Our DPC is Mrs Debbie Tran, and she can be contacted at *dpc@cfschool.org.uk*

The DPC together with senior management and Governors, is responsible for ensuring compliance with the Data Protection Legislation and with this policy with support from Jucicium Education, our DPO. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPC.

The DPC is also the central point of contact for all **data subjects** and others in relation to matters of data protection.

- **All Staff**

○ Be aware of and comply with this policy, attending training and reporting concerns.

○ Seek advice from the person responsible for handling that type of data before sharing any personal, sensitive or confidential information.

5. Data protection principles

Anyone **processing personal data** must comply with the data protection principles. These provide that **personal data** must be:

- **processed** fairly and lawfully and transparently in relation to the **data subject**
- **processed** for specified, lawful purposes and in a way, which is not incompatible with those purposes
- adequate, relevant and not excessive for the purpose
- accurate and up to date
- not kept for any longer than is necessary for the purpose
- **processed** securely using appropriate technical and organisational measures.

Personal data must also:

- be **processed** in line with **data subjects'** rights
- not be transferred to people or organisations situated in other countries without adequate protection.

We will comply with these principles in relation to any **processing** of **personal data** by the school.

6. Fair and lawful processing

Data Protection legislation is not intended to prevent the **processing** of **personal data**, but to ensure that it is done fairly and without adversely affecting the rights of the **data subject**.

For **personal data** to be **processed** fairly, **data subjects** must be made aware:

- that the **personal data** is being **processed**
- why the **personal data** is being **processed**
- what the lawful basis is for that **processing** (see below)
- whether the **personal data** will be shared, and if so with whom
- the period for which the **personal data** will be held
- the existence of the **data subject's** rights in relation to the **processing** of that **personal data**

- the right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

We will only obtain such **personal data** as is necessary and relevant to the purpose for which it was gathered and will ensure that we have a lawful basis for any **processing**.

For **personal data** to be **processed** lawfully, it must be **processed** on the basis of one of the legal grounds set out in the Data Protection legislation. We will normally **process personal data** under the following legal grounds:

- where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract
- where the **processing** is necessary to comply with a legal obligation that we are subject to, (e.g. the Education Act 2011)
- where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest
- where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **personal data.**
- When **special category personal data** is being processed then an additional legal ground must apply to that processing. We will normally only **process special category personal data** under following legal grounds:
    - where the **processing** is necessary for employment law purposes, for example in relation to sickness absence
    - where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment
    - where the **processing** is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities
    - where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **special category personal data**.

We will inform **data subjects** of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.

If any **data user** is in doubt as to whether they can use any **personal data** for any purpose, then they must contact the DPC before doing so.

Vital Interests

There may be circumstances where it is considered necessary to **process personal data** or **special category personal data** in order to protect the vital interests of a **data subject**. This might include medical emergencies where the **data subject** is not in a position to give consent to the **processing**. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPC in advance, although there may be emergency situations where this does not occur.

Consent

Where none of the other bases for **processing** set out above apply then the school must seek the consent of the **data subject** before **processing** any **personal data** for any purpose.

There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.

When pupils and or our **workforce** join Christian Fellowship School a consent form will be required to be completed in relation to them. This consent form includes but is not limited to the taking and use of photographs and videos of them, and consent to add pupils to digital platforms necessary for their education. Where appropriate third parties may also be required to complete a consent form.

In relation to all pupils in Lower School and Middle School we will seek consent from an individual with parental responsibility for that pupil.

We will seek consent directly from pupils in Upper School and inform parents, however we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from an individual with parental responsibility.

If consent is required for any other **processing** of **personal data** of any **data subject,** then this consent must:

- inform the **data subject** of exactly what we intend to do with their **personal data**
- require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in
- inform the **data subject** of how they can withdraw their consent.
- Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a **data subject** giving their consent.
- Certain services such as Google Workspace are considered to be essential for the education of pupils - in consequence consent in respect of **personal data** associated with Google Workspace is a condition of all pupils joining the school.

The DPC must always be consulted in relation to any consent form before consent is obtained.

A record must always be kept of any consent, including how it was obtained and when.

7. Processing for limited purposes

In the course of our activities Christian Fellowship School may collect and **process** the **personal data** set out in our Schedule of Processing Activities. This may include **personal data** we receive directly from a **data subject** (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and **personal data** we receive from other sources (including, for example, local authorities, other schools, parents, other pupils or members of our **workforce**).

We will only **process personal data** for the specific purposes set out in our Schedule of Processing Activities or for any other purposes specifically permitted by Data Protection legislation or for which specific consent has been provided by the data subject.

8. Notifying data subjects

If we collect **personal data** directly from **data subjects**, we will inform them about:

- our identity and contact details as **Data Controller** and those of the DPC
- the purpose or purposes and legal basis for which we intend to **process** that **personal data**
- the types of third parties, if any, with which we will share or to which we will disclose that **personal data**

- whether the **personal data** will be transferred outside the European Economic Area ('**EEA**') and if so the safeguards in place
- the period for which their **personal data** will be stored, by reference to our Retention and Destruction Policy
- the existence of any automated decision making in the **processing** of the **personal data** along with the significance and envisaged consequences of the **processing** and the right to object to such decision making
- the rights of the **data subject** to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.
- Unless we have already informed **data subjects** that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive **personal data** about a **data subject** from other sources, we will provide the **data subject** with the above information as soon as possible thereafter, informing them of where the **personal data** was obtained from.

Christian Fellowship School will be provided with information relating to third parties in the form of emergency contact details. These individuals must be provided with the information above. Practically we suggest that parents are required to obtain the consent of any third party whose details they provide to the school for these purposes.

9. Adequate, relevant and non-excessive processing

We will only collect **personal data** to the extent that it is required for the specific purpose notified to the **data subject**, unless otherwise permitted by Data Protection Legislation.

10. Accurate data

- We will ensure that **personal data** we hold is accurate and kept up to date.
- We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

Data subjects have a right to have any inaccurate **personal data** rectified. See further below in relation to the exercise of this right.

11. Timely processing

We will not keep **personal data** longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all **personal data** which is no longer required.

12. Processing in line with data subject's rights

- We will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:
- request access to any **personal data** we hold about them
- object to the **processing** of their **personal data**, including the right to object to direct marketing
- have inaccurate or incomplete **personal data** about them rectified
- restrict **processing** of their **personal data**
- have **personal data** we hold about them erased
- have their **personal data** transferred
- object to the making of decisions about them by automated means.

The Right of Access to Personal Data

Data subjects may request access to all **personal data** we hold about them. Such requests will be considered in line with the schools Subject Access Request Procedure.

The Right to Object

In certain circumstances **data subjects** may object to us **processing** their **personal data**. This right may be exercised in relation to **processing** that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

An objection to **processing** does not have to be complied with where the school can demonstrate compelling legitimate grounds which override the rights of the **data subject**.

Such considerations are complex and must always be referred to the DPC upon receipt of the request to exercise this right.

In respect of direct marketing any objection to **processing** must be complied with.

Christian Fellowship School is not however obliged to comply with a request where the **personal data** is required in relation to any claim or legal proceedings.

The Right to Rectification

If a **data subject** informs the Christian Fellowship School that **personal data** held about them by Christian Fellowship School is inaccurate or incomplete, then we will consider that request and provide a response within one month.

If we consider the issue to be too complex to resolve within that period, then we may extend the response period by a further two months. If this is necessary, then we will inform the **data subject** within one month of their request that this is the case.

We may determine that any changes proposed by the **data subject** should not be made. If this is the case, then we will explain to the **data subject** why this is the case. In those circumstances we will inform the **data subject** of their right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

The Right to Restrict Processing

Data subjects have a right to 'block' or suppress the **processing** of **personal data**. This means that Christian Fellowship School can continue to hold the **personal data** but not do anything else with it.

Christian Fellowship School must restrict the **processing** of **personal data**:

- where it is in the process of considering a request for **personal data** to be rectified (see above)
- where the Christian Fellowship School is in the process of considering an objection to processing by a **data subject**
- where the **processing** is unlawful, but the **data subject** has asked Christian Fellowship School not to delete the **personal data**
- where the Christian Fellowship School no longer needs the **personal data,** but the **data subject** has asked the Christian Fellowship School not to delete the **personal data** because they need it in relation to a legal claim, including any potential claim against Christian Fellowship School.

If Christian Fellowship School has shared the relevant **personal data** with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

The DPC must be consulted in relation to requests under this right.

The Right to Be Forgotten

Data subjects have a right to have **personal data** about them held by Christian Fellowship School erased only in the following circumstances.

- Where the **personal data** is no longer necessary for the purpose for which it was originally collected.
- When a **data subject** withdraws consent – which will apply only where the Christian Fellowship School is relying on the individual's consent to the **processing** in the first place.
- When a **data subject** objects to the **processing** and there is no overriding legitimate interest to continue that **processing** – see above in relation to the right to object.
- Where the **processing** of the **personal data** is otherwise unlawful.
- When it is necessary to erase the **personal data** to comply with a legal obligation.
- If Christian Fellowship School offers information society services to a pupil and consent is withdrawn in respect of that pupil in relation to those services.

The Right to Data Portability

In limited circumstances a **data subject** has a right to receive their **personal data** in a machine-readable format, and to have this transferred to another organisation.

If such a request is made, then the DPC must be consulted.

13. Data security

We will take appropriate security measures against unlawful or unauthorised processing of **personal data**, and against the accidental loss of, or damage to, **personal data**.

We will put in place procedures and technologies to maintain the security of all **personal data** from the point of collection to the point of destruction.

Security procedures include:

Entry controls. Any unauthorised person seen unsupervised in areas containing confidential information should be reported to the DPC or Head Teacher

Secure lockable desks, cupboards or rooms. Desks, cupboards or rooms should be kept locked when unattended if they hold confidential information of any kind. (Personal information is always considered confidential.) For information on how this is to be implemented please see GDPR implementation schedule.

Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets.

Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off or lock their PC when it is left unattended.

Working away from the school premises – paper documents.
Unless required for the exercise of professional duties, paper documents containing personal data should not be taken away from the school premises.
Working away from the school premises – electronic working.
Documents should be password protected and Data users must ensure that their home monitors do not show confidential information to passers-by (inc. close family members) and that they log off or lock their PC when it is left unattended.
For more details please refer to the school e-safety policy
Document printing. Documents containing **personal data** must be collected immediately from printers and not left on photocopiers.

Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

14. Data Protection Impact Assessments

Christian Fellowship School takes data protection very seriously and will consider and comply with the requirements of Data Protection Legislation in relation to all its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

In certain circumstances the law requires us to carry out detailed assessments of proposed **processing**. This includes where we intend to use new technologies which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing** or the way that we intend to do so.

Christian Fellowship School will complete an assessment of any such proposed **processing** and has a template document which ensures that all relevant matters are considered.

The DPC should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

In normal circumstances, a DPIA "request" (using the DPIA Request Template) will be submitted by the relevant staff member with guidance from the DPC. Section 5 of the template outlines the known or perceived risks, while Section 6 assesses the mitigation and the residual risk. Following this, Section 7 (Authorisation) is completed by a designated member of the senior staff team - at the time of this Policy this is the role of the Business Manager.

15. Disclosure and sharing of personal information

We may share **personal data** that we hold about **data subjects**, and without their consent, with other organisations. Such organisations include the Department for Education, [and / or Education and Skills Funding Agency ESFA], Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, Unifrog, Century Tech and other organisations where we have a lawful basis for doing so.

Christian Fellowship School will inform **data subjects** of any sharing of their **personal data** unless we are not legally required to do so, for example where **personal data** is shared with the police in the investigation of a criminal offence.

In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy.

Further detail is provided in our Schedule of Processing Activities.

16. Data processors

We contract with various organisations who provide services to Christian Fellowship School, including but not limited to:

Sage payroll, Pupil Asset, examination boards, photographer, GL-Assessments (CAT tests), Unifrog, Abacus, My Maths, Century Tech, Turing Scheme

In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.

Personal data will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of Christian Fellowship School. Christian Fellowship School will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.

Contracts with **data processors** will comply with Data Protection Legislation and contain explicit obligations on the **data processor** to ensure compliance with the Data Protection Legislation, and compliance with the rights of **Data Subjects**.

17. Images and videos

Parents and others attending Christian Fellowship School events can take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a school performance involving their child. Christian Fellowship School does not prohibit this as a matter of policy.

Christian Fellowship School does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Christian Fellowship School to prevent.

Christian Fellowship School asks that parents and other members of the school community do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

At Christian Fellowship School we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents where appropriate; usually at the beginning of each academic year or when the pupil joins the school; before allowing the use of images or videos of pupils for such purposes.

Whenever a pupil begins their attendance at Christian Fellowship School they, or their parents where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent. This consent will also be sought again at the beginning of each academic year.

CCTV

Christian Fellowship School operates a CCTV system. Please refer to the Christian Fellowship School CCTV Policy.

18. Changes to this policy

We may change this policy at any time. Where appropriate, we will notify **data subjects** of those changes.

APPENDIX A: DEFINITIONS

Term	Definition
Data	Information which is stored electronically, on a computer, or in certain paper-based filing systems.
Data Subjects	For the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
Personal Data	Any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Controllers	The people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes.
Data Users	Those of our workforce (including governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
Data Processors	Any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
Processing	Any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.
Special Category Personal Data	Information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.
Workforce	Includes any individual employed by Christian Fellowship School such as staff and those who volunteer in any capacity including governors [and/or trustees / members/ parent helpers].