

CFBL Privacy Notice for Staff* & Governors

(*Applicable to all current and former staff, volunteers, staff of contractors, and to job applicants)

Authorised by:	The Board of Governors of CFBL
Date:	WR 21 January 2026
Review frequency:	<u>Annually</u> or following any updates to relevant laws and regulations
Next review:	January 2027
Circulation:	Governors/all staff/volunteers, automatically Staff: Shared drive > Staff > HR > HR policies and Shared drive > Staff > Policies School Website

In the course of your employment, engagement or other basis of work undertaken for the School, we will collect, use and hold ("process") personal data relating to you. We will also process your personal data when you apply for a role with CFBL. This Privacy Notice sets out how we will use that information in accordance with the UK General Data Protection Regulation, the Data Protection Act 2018, the Data Use and Access Act 2025, and supporting legislation (together, "**Data Protection Law**"). It also sets out what your rights as staff, applicants or governors are in relation to your personal data.

This Privacy Notice should be read in conjunction with CFBL's Privacy Notice Applicable to all Members of the School Community (past and present), which complements it. In the event of any conflict or inconsistency between this Privacy Notice for Staff & Governors and CFBL's Privacy Notice Applicable to all Members of the School Community (past and present), this Privacy Notice for Staff & Governors will take precedence for staff (as defined below).

1. Who this document applies to

This document applies to:

- teaching and other staff, contractors, itinerant teachers, casual workers, temps and volunteers who may be employed or engaged by the School to work for it in any capacity,
- prospective applicants for roles,
- the School's governors/trustees /directors (including former governors/trustees/directors),

referred to collectively as '**staff**' in this Staff & Governors Privacy Notice (this '**Privacy Notice**'), with respect to data processed by the School in relation to their employment or the work that they undertake for or on behalf of the School.

This notice is not aimed at pupils, or parents of pupils (whether current, past or prospective) or other members of the public, nor does it inform staff how to handle the personal data of the same.

2. About this document

The School is the data controller for your personal information. This means that the School is responsible for deciding what personal information we collect, hold and use about you. The School is also responsible for deciding how and why that personal information is used.

This Privacy Notice explains how the School processes personal data of staff, and your rights in relation to the personal data we hold.

All staff must read this Privacy Notice, together with the School's other relevant policies and any documents containing terms and conditions related to data privacy, including, without limitation:

- the School's Privacy Notice for All Members of the School Community;
- any contract between the School and its staff, such as the terms and conditions of employment;
- any applicable staff handbook and HR intranet;
- the School's CCTV policy;
- the School's document retention policy;
- the School's safeguarding and health and safety policies, including as to how concerns or incidents are reported or recorded (both by and about staff);
- the School's IT policies, including its Use of Telephone, Email Systems and Internet policy for staff; and
- any information provided on an ad hoc basis when collecting particular personal data for a specific use, for example, when collecting data via an online or paper form.

Please note that your contract with the School, including any document or policy forming part of your contractual obligations to the School, may, in particular, be relevant to and supplement the information in this Privacy Notice, to the extent that it will contain details of obligations or rights of the School under contract with you which may require the use of your personal data. However, this Staff Privacy Notice is the primary document applicable to the use of your personal data by the School.

This Privacy Notice does not form part of any contract of employment or other contract for services, and we may amend it at any time.

3. How we collect your information

We collect most of your personal information directly from you. Depending on whether you are an employee, worker, contractor, applicant or governor, we may also collect your information from other sources.

For example, we may collect your personal data:

- from the information you provide to us before making a formal job application, for example, from your curriculum vitae;
- from social networking sites, as part of background checks carried out on you by the School under the School's Safer Recruitment Policy;
- when you submit a formal application to work for us, and provide your personal data in application forms and covering letters, etc.;
- from third parties, for example, the Disclosure and Barring Service (DBS) and referees (including your previous or current employers or school), in order to verify details about you and/or your application to work for us; and
- from other members of staff or from parents/pupils, in order to investigate and/or resolve incidents or concerns raised as part of your employment or engagement with us.

More generally, if you work for us, then we will also process data you provide or create during the course of your employment or engagement, including:

- when you provide or update your contact details;
- if you are an employee, when you or another member of staff completes paperwork regarding your performance appraisals;
- in the course of fulfilling your employment, engagement or equivalent duties more generally, including by filling reports, note-taking, or sending emails on School systems;
- in various other ways as you interact with us during your time as a member of staff, and afterwards, where relevant, for the various purposes set out below.

4. The types of personal data we collect, store and use

(i) About all staff, including applicants (whether or not successful in their application):

- personal contact and communications information, including:
 - your name, title and gender
 - your contact details (including email address(es), telephone numbers and postal address(es));

- o records of communications and interactions we have had with you;
- recruitment and work history information, including:
 - o if applying for or working in a role as an employee or worker, a copy of your CV, interview notes, application forms, details of your education and references from your institutions of study, references from your previous employer(s) and other information collected as part of the application process;
 - o if applying for or working in a role as a contractor or volunteer, information about your work experience, such as previous roles held, or projects worked on, qualifications, notes from discussions relevant to the work required and any other information collected as part of the application process; or
 - o if applying for or working in a role as a governor/trustee/director, your personal statement for elections, your resumé, information about your work experience, qualifications, notes from discussions relevant to the work required and any other information collected as part of the application and appointment process;

(ii) About all staff, except unsuccessful applicants:

This includes some or all of the following, depending on your role:

- contractual terms and conditions (including any updated or amended terms);
- personal data from background checks, including DBS and foreign criminal checks, teaching regulation checks, and for the management team, absence of disqualifications to act as manager or proprietor of a charity and s128 checks;
- work-related information, including:
 - o your personal data captured in the work product(s), notes and correspondence you create while employed by or otherwise engaged to work for the School;
 - o details of your professional activities and interests;
 - o details of training;
 - o details of regulatory declarations made by you (for example, where you are being asked to confirm that you read certain guidance or policies);
 - o details of incidents or concerns or complaints relating to you, made under the School's safeguarding policies or other School policies;
 - o your involvement with and membership of sector bodies and professional associations;
 - o information about and linked to your use of our information and communications systems (including emails, telephone records, Google Suite, Microsoft Teams, Slack, Webex).
- CCTV footage;
- Security access card records;
- your image and likeness, including as captured in photographs taken for work purposes.

(iii) About employees and workers.

This includes some or all of the following, depending on whether you are an employee or a worker:

- financial information, including:
 - o your bank account number(s), name(s) and sort code(s) (used for paying your salary and/or processing other payments);
 - o your tax status (including residence status);
 - o remuneration information (including salary for employees);
 - o if you are an employee, information related to pensions, national insurance, or employee benefit schemes.
- biographical, educational and social information, including nationality, date of birth, right to work in the UK and visa.
- Next of kin and emergency contact information.
- Marital status and dependents, when listed as beneficiaries for employee benefits.

- Variable or discretionary remuneration (such as bonuses, commission payment, etc.)
- Annual leave entitlement and records.
- Other leave information (such as jury duty, compassionate leave, study leave) (including dates and any pay).
- Date of continuous employment.
- Working time documentation (including opt-out forms and records showing compliance).
- PAYE records.
- Employment records (including job titles, promotion/demotion records, training records and professional memberships).
- Compensation history (including salary review and bonus award letters).
- Performance management information (including appraisals, meeting notes, PIP documentation, etc.).
- Disciplinary and/or grievance information (including meeting notes, invitation letters, reports, outcome letters and formal warnings).
- Jobs, volunteering or other activities that you carry out outside your job or services for the School.

Where necessary for your employment or other engagement to work for us, we also collect, store and use special categories of data, including:

- information revealing your racial or ethnic origin (e.g., your passport or other photographic documentation);
- trade union membership, where applicable;
- information concerning your health and medical conditions (for example, to ensure your fitness to teach, where required to monitor and record sickness absences, dietary needs, to make reasonable adjustments to your working conditions or environment or in relation to an absence management process); and
- Information concerning or implying your sexual life or orientation (for example, maternity or other family leave documentation such as MAT1B, maternity pay, pregnancy risk assessments and other family leave dates and pay, equal opportunity questionnaire).

(iv) About contractors

This includes some or all of the following:

- financial information, including:
 - bank account number(s), name(s) and sort code(s) (used for processing payments);
- date of birth and copy of passport;
- Information for SCR: DBS, teaching agency checks etc.

(v) About governors.

- your bank account number(s), name(s) and sort code(s) (used to sign you up as an approved bank signatory).
- Your NI number (used for the DfE annual census).
- Copy of passport.
- Copy of utility bills (used for KYC obligations).
- Section 128 check and other checks with Companies House and the Charity Commission to confirm your capacity and suitability to act as a proprietor, director and trustee of the School.
- DfE check and approval to act as Chair of the board.

Where necessary for your role, we also collect, store and use special categories of data, including:

- information revealing your racial or ethnic origin (e.g., your passport or other photographic documentation).

5. How your personal data is used and the legal basis for processing

We will only use your personal data when we are allowed to under the Data Protection Law. The most common reasons for using your personal data are set out below. Some of these reasons will overlap, and there may be several reasons we use your personal data.

We will only use your personal information for the reason we first collected it, unless we reasonably think we can use it for another, compatible purpose. If we use your personal information for another, unrelated purpose, we will notify you and explain the reason why.

(i) Entering into, or fulfilling, our contract with you

We process your personal data because it is necessary for the performance of a contract to which you are a party or in order to take steps at your request prior to entering into a contract, such as a contract of employment or engagement with us. In this respect, we use your personal data for the following reasons:

- administering job applications and, where relevant, negotiating and entering into a contract with you;
- unless you are a volunteer or governor, to pay you and (if you are an employee) to administer benefits (including pensions) under your contract;
- if you are an employee, managing your contractual entitlement to annual leave and pay, as well as any contractual sickness absence pay you are entitled to;
- If you are an employee, managing potential conflicts with outside interests; and
- managing arrangements for the termination of our working arrangements, such as issuing or processing any notice requirements or other obligations (such as the return of School property).

(ii) Legitimate Interests

We process your personal data because it is necessary for our (or sometimes a third party's) legitimate interests, provided your interests and rights do not override those legitimate interests. In this respect, we use your personal data for the following:

- for security purposes, including by operating security cameras in various locations on the School's premises;
- to enable relevant authorities to monitor the School's performance and to intervene or assist with incidents as appropriate;
- If you are a non-British employee, to sponsor a skilled worker's visa;
- if you are an employee, to set performance requirements for your role and reviewing and managing your performance;
- for the purposes of management planning and forecasting, research and statistical analysis;
- in connection with organising events and social engagements for staff, including making travel arrangements on your behalf;
- to monitor (as appropriate) use of the School's IT and communications systems in accordance with the School's Use of Telephone, Email Systems, and Internet Policy and government guidance such as KCSIE; and
- to deal with any actual or prospective legal disputes involving you or another individual.

(iii) Legal Obligations

We also process your personal data where we need to for our compliance with a legal obligation, notably those in connection with employment, charity/company law, tax, accounting, and child welfare. In this respect, we use your personal data for the following:

- if you are an employee or worker, checking that you have the legal right to work in the UK;
- If you are a sponsored employee, ensuring compliance with the CFBL immigration licence;
- checking any restrictions to work in our School that may apply to you (eg - DBS and other criminal record checks, teaching agency checks, section 128 checks, Companies House and Charity Commission checks etc);
- determining your tax status and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions;

- complying with our health and safety obligations;
- to safeguard pupils' welfare and provide appropriate pastoral care;
- if you are working as a teacher or support staff, complying with our obligation to ensure you are medically fit to teach;
- if you are an employee, managing your statutory sick leave entitlements and complying with our associated obligations;
- if you are an employee, managing and administering your statutory entitlement to annual leave and other statutory leave (such as maternity, paternity or other family leave);
- if you are an employee, monitoring compliance with working time requirements (such as the 48-hour maximum working week);
- if you are an employee, enrolling you in a pension arrangement as required under the Pensions Act 2008;
- if you are an employee, managing grievance and/or disciplinary processes;
- if you are an employee, maintaining PAYE, payroll and working time records in accordance with statutory minimum retention requirements;
- If you are a governor/trustee/director, managing your ability to act as a governor/trustee/director, managing conflicts of interests;
- to carry out or cooperate with any School or external complaints, disciplinary or investigatory process;
- reporting and cooperating with the police or other competent authorities, for the prevention and detection of crime, and in order to assist with investigations (including criminal investigations) carried out by the police and other competent authorities.

(iv) Special categories of data

Special categories of more sensitive personal information require additional protection, and we need to meet additional conditions to be able to process it. Further information about the measures we take when using staff special category data is set out in our Data Protection Policy, located on the shared drive > Staff > HR > HR policies.

We may process your special category personal data in the following circumstances:

- if you are an employee or worker, where necessary to carry out our obligations and/or exercise our or your specific rights under employment law. This includes checking your right to work in the UK, assessing your fitness to teach or, for employees only, monitoring and managing your sickness absence and administering statutory leave and benefits (such as maternity leave and pay);
- where necessary for reasons of substantial public interest, such as equal opportunities monitoring or, in certain circumstances, the safeguarding of children;
- where necessary in relation to an actual or potential legal dispute involving you or another individual. This would include information needed for court proceedings and/or to obtain legal advice; and/or
- in limited circumstances, with your explicit written consent.

There may be other, less likely circumstances where we need to process your special category data. For example, we may process this type of information where you have already made it public or if necessary to protect the vital interests (those essential for life) of you or another person, and you are incapable of giving your consent. One example might be where you or someone else needs urgent medical care.

Consent

We do not need your consent to use your personal data where we are otherwise permitted to process it under Data Protection Law. We also do not need your consent to process your special category data, as long as we meet one other additional condition under the Data Protection Law.

In limited circumstances, we may approach you to ask for your specific and written consent to allow us to use certain types of data. If this happens, we will provide you with full details of the information we want to use and the reason we need it, so you can carefully consider whether you wish to consent.

It is not a condition of your employment or other contract with us that you agree to any request for consent that might be made by us. Where you have provided consent, you can withdraw it at any time.

Criminal offence data

We process information about certain criminal convictions and offences, where necessary, based on the nature of your role and in compliance with our legal and regulatory obligations. We will collect this information as part of the recruitment process (criminal records checks). We may also be notified of such information directly by you in the course of your working for the School.

We will use criminal offence data to comply with our legal and regulatory obligations, which include:

- ensuring that you are permitted to teach, undertake regulated activity relating to children, or otherwise perform your role and that you are not barred from doing so, and checking whether you have previously been dismissed for reasons linked to the hard of a child;
- recording and/or reporting certain allegations made (including to the police or other authorities); and
- notifying the DBS about certain behaviour.

We will only process criminal offence data where we also meet an additional condition. The most common reasons are that the processing is necessary for the prevention or detection of an unlawful act or for the safeguarding of children.

Criminal offence data is particularly sensitive and subject to additional protections under the Data Protection Law. Further information about the measures we take when using criminal offence data is set out in our Data Protection Policy, located on the shared drive > Staff > HR > HR policies.

6. Sharing your information with others

For the purposes referred to in this Privacy Notice and relying on the basis for processing as set out above, we may share your personal data with certain third parties. We may disclose limited personal data (including in limited cases, special category or criminal data) to a variety of recipients including:

- Third-party service providers, to carry out activities on our behalf including:
 - o payroll – ePayslips
 - o IT services: Every HR, 1Password
 - o pension administration – via AVIVA or TPT
 - o criminal records check - Carechecks
 - o CCTV - HikVision
 - o providing and administering benefits - Perkbox, HSF, Bike to work, Borker Mercer Life Insurance
- Third party authorities where necessary to meet a legal or regulatory obligation, such as HMRC, UKVI, the Home Office, DBS, the Department for Education, the Information Commissioner's Office, Charity Commission, Companies House, the local authority, the Teaching Regulation Agency and/or the police.
- Where necessary for training purposes or to meet legal or regulatory obligations as a French-accredited (*homologuée*) school, the EFE, MLF, AEFE, the French Embassy Service Culturel, the French Embassy security services.
- External auditors or inspectors (including, without limitation, French MEN and OFSTED inspectors).
- Our third-party advisers, where it is necessary for us to obtain their advice or assistance, including insurers, lawyers, accountants, auditors or other external consultants.
- Other third parties in specific and more limited circumstances, such as KTECT in the context of the appointment of Non-Parent Trustees or the Chair / Treasurer, or we are extending our School.
- The School's bank under KYC or other compliance requirements.

We may also share information about you with other employers in the form of a reference, where we consider it appropriate, or if we are required to do so in compliance with our legal obligations.

7. International Transfers

We transfer staff personal information to the following countries outside the UK:

- Google Workspace: Dublin, Republic of Ireland
- Eduka: Europe (Netherlands)

8. How long is your information kept

Personal data relating to unsuccessful job applicants is deleted within one year of the end of the application process.

For employees, subject to any other notices that we may provide to you, we will normally retain your personal data for a period of six years after your contract of employment (or equivalent agreement) has expired or been terminated. However, some information may be retained for longer than this, for example, incident reports and safeguarding files, in accordance with specific legal requirements. Please refer to our Document Retention Policy available from the School's shared drive > Staff > Policies for more details.

For trustees, workers, contractors and volunteers, please refer to our Document Retention Policy.

9. Automated decision making

Automated decision-making takes place when an electronic system uses personal information to make a decision without any human intervention. We do not envisage that any decisions will be taken about you using automated means, but will notify you if this changes.

10. Your rights

Please see our Privacy Notice for All Members of the School Community (past and present), which has details of your rights as a 'data subject'. A copy of it is available on the shared drive > Staff > Policies or from the School's website. You can find out more about your rights under applicable data protection legislation from the Information Commissioner's Office website available at www.ico.org.uk.

If you wish to exercise any of your data rights, please contact the Data and Systems Manager in writing (dataprotection@cfbl.org.uk) in the first instance.

11. Data accuracy

Staff members must update their details directly on the platform providing payroll (e.g. EveryHR/ePayslip or such other platforms that may replace them) or pension services, and inform the HR Department accordingly. If the information concerned is not on said platform, please contact HRqueries@cfbl.org.uk. The School will remind employees every 6 months via the HR newsletter to check if their details on Every HR are up to date (address, next of kin, phone number, personal email address and bank details).

12. Updates

The School will update this Privacy Notice from time to time. Any substantial changes that affect your rights will be provided to you directly as far as is reasonably practicable.

13. Contact and complaints

Any comments or queries on this Privacy Notice or how we handle your personal information should be directed to the Data and Systems Manager at dataprotection@cfbl.org.uk in the first instance.

In addition, the School uses the services of a Data Protection Officer. The Data Protection Officer is responsible for overseeing data protection within the School. If you have any questions about how we handle your personal information which cannot be resolved by the Data & Systems Manager, then you can contact the DPO at:

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 (Option 1, then 1)

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO) with respect to data protection issues.

Last review by management and data & systems trustees: January 2026

Previous Versions:

17.05.18

21.09.20

15.11.22

29.04.25

Current

Document Owner and Approval

The Legal Manager is the owner of this document and is responsible for ensuring that it is reviewed in line with the School's policy review schedule.