STAFF PRIVACY NOTICE

1. What is the purpose of this document?

EFL Trust are committed to protecting the privacy and security of your personal information. The two organisations work together in the processing and management of employee data.

This privacy notice describes how EFL Trust process personal information about you during and after your working relationship with us, in accordance with data protection legislation.

It applies to all employees, workers, trustees and contractors.

EFL Trust are a data controller. This means that we are responsible for making decisions about the personal data that we process.

This notice applies to current and former employees, workers, trustees and contractors. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

2. Where do we obtain your personal data from?

The sources of information we process about you:

- From the EFL (for example, where they process your application on our behalf)
- Directly from you
- From an employment agency
- From your employer (for example, if you are on secondment)
- From referees
- From an organisation completing background checks
- From CCTV (from EFL, where they are the data controller for our premises)
- From Occupational Health/ other health providers
- From Pension administrators and/or providers of any staff benefits
- From HMRC (for tax purposes)

3. What kind of information do we hold about you, and why?

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where an individual can not be identified (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection.

We will process the following categories of personal information about you:

Information relating to the recruitment process, to enable us to make a business decision about your potential recruitment, and contact your regarding your application:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Recruitment information (including copies of right to work documentation, references and other information included in your application form, CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).

Information relating to your employment, in order for us to perform HR processes, and to enable us to carry out our contract with you:

- Personal contact details such as name, title, addresses, telephone numbers, and email addresses.
- Date of birth.
- Gender.
- Marital status and dependents.
- Next of kin and emergency contact information.
- National Insurance number.
- Proof of identity and/or address.
- Start date and end date.
- Location of employment or workplace.
- Any secondary employment and conflicts of interest.
- Information about criminal convictions and offences

Information about your salary and work-related benefits, to allow us to pay you correctly, provide you with work-related benefits, and administer statutory entitlements:

- Start and end date.
- Salary information, including pay grade and working pattern, expenses, and any maternity/paternity/adoption pay details.
- Annual leave, and any other leave requests
- Pension, life assurance and benefits information.

- Copy of driving license, insurance, MOT and any other documents concerning business driving.

Performance information, in order to carry out our performance management policy (such as completing appraisals), conducting pay reviews, dealing with disputes, and meeting your training needs:

- Disciplinary and grievance information (such as warnings, and records of hearings, including instances where you may be a witness).
- Appraisal records.
- Requests for training, and training records.
- Information relating to your development and support (for example, work plans, performance improvement plans, records of meetings where performance was discussed).
- Whilsteblowing information.

Monitoring Information, to allow us to assess compliance with internal policies and maintain the safety of you and/or others:

- CCTV footage and other information obtained through electronic means such as swipecard records (information shared by EFL).
- Information about your use of our information and communications systems (including emails).
- Photographs.
  Although monitoring information may be used for investigations, including disciplinary and grievance procedures, and compliance against internal policies, we do not carry out routine monitoring of ICT usage or CCTV.

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, disability status, gender identification, and/or sexual orientation for equal opportunities monitoring.
- Information about your health, including any medical condition, health and sickness records, occupational health referrals, and records of any work-related accidents.

In addition to this, we process information about criminal convictions and offences, where your role requires us to do so. If your role requires a criminal records check (DBS), we will not keep a copy of your DBS check. We will keep a record of the outcome of such checks, that indicates whether you have satisfied our safer recruitment checks.

4. How will this information be processed lawfully?

We will only process personal information when the law allows us to. Depending on the processing activity, we rely on the following lawful bases:

1. Article 6(1)(b), Where we need to perform the contract we have entered into with you
2. Article 6(1)(c), Where we need to comply with a legal obligation
3. Article 6(1)(d), Where we need to protect your vital interests, or those of somebody else, and you are incapable of providing consent.
4. Article 6(1)(f)Where it is necessary for our legitimate interests, your legitimate interests, or those of a third party, and your interests and fundamental rights do not override those interests

The lawful basis we rely upon for processing your data is related to the purpose of the processing. We have indicated below with asterisks where each lawful basis will apply.

- Making a decision about your recruitment or appointment.***
- Determining the terms on which you work for us.***
- Assessing qualifications and suitability for a particular role, job or task, including decisions about promotions.***
- Checking you are legally entitled to work in the UK.**
- Paying you and reimbursing expenses*
- Deducting tax and National Insurance contributions.**
- Providing work-related benefits to you: such as private medical care plan, life assurance, company cars and / or any other benefit that may be provided from time to time.*
- Liaising with your pension provider.*
- Administering the contract we have entered into with you.*
- Business management and planning, including accounting and auditing.***
- Conducting performance reviews, managing performance and determining performance requirements. Carrying out our performance management policy (such as completing appraisals), conducting pay reviews, dealing with disputes, and meeting your training needs ***
- Making decisions about salary reviews and compensation.***
- Processing of evidence and information relating to grievance or disciplinary hearings.**
- Making decisions about your continued employment or engagement.***
- Making arrangements for the termination of our working relationship.***
- Education, training and development requirements.***
- Complying with regulatory obligations. E.g. recording information, such as incidents and accidents at work, that we have a legal obligation to record.**
- Dealing with civil legal disputes involving you, or other employees, workers and contractors, including accidents at work.***
- Where a legal dispute compels us to process (such as a court order). **
- Ascertaining your fitness to work.**
- Managing sickness absence.***

- To prevent fraud.**
- Monitoring Information, to allow us to assess compliance with internal policies and maintain the safety of you and/or others.***
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.***
- To conduct data analytics studies to review and better understand employee retention and attrition rates.***
- Equal Opportunities and Diversity monitoring.**
- Ensuring your eligibility to drive for business purposes.***
- Ensuring you are able to work with vulnerable adults or under 18's (where applicable).**

** necessary to perform our contract with you.*
*** to enable us to comply with legal obligations.*
**** to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. Our legitimate interests may include the ensuring the efficient operation, improvement and administration of the business, protecting its integrity and/or rights (or those of others).*

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

Special category data:

We will use your special category information for:

- Ascertaining your fitness to work
- Managing sickness absence
- Equal Opportunities and Diversity monitoring

In order to process special categories of information about you, we are also required to meet a further lawful basis for processing. The lawful bases relied upon for this are:

- Article 9(2)(a), where you have provided your unambiguous, explicit consent
- Article 9(2)(b) which relates to carrying out our obligations and exercising our rights in employment and the safeguarding of your fundamental rights.
- Article 9(2)(c) to protect your vital interests or those of somebody else, where you are incapable of giving your consent.
- Article 9(2)(f) for the establishment, exercise or defense of legal claims.
- Article 9(2)(g) processing is necessary for reasons of substantial public interest (subject to safeguards and proportionate to your rights).
- Article 9(2)(h) for the purposes of preventative or occupational
- medicine and the assessment of your working capacity as an employee.

Some of those conditions for processing special category data also require us to rely on a further lawful basis for processing under the Data Protection Act 2018 (DPA 18). We further rely on:

- Schedule 1 Part 1 of the DPA 18:

- Paragraph 1 – Purpose: the processing for employment purposes. (Related to Article 9(2)(b)).
  Paragraph 2(2)(a) and (b) – Purpose: the processing for preventative or occupational medicine and the assessment of the working capacity of an employee (Related to article 9(2)(h)).
- Schedule 1 Part 2 of the DPA 18:
  - paragraph 8 – Purpose: equality of opportunity or treatment (Related to article 9(2)(g))
  - paragraph 9 – Purpose: racial or ethnic diversity at senior levels of organisation (Related to article 9(2)(g))
  - paragraph 16 – Purpose: support for individuals with a particular disability or medical condition (Related to article 9(2)(g))
  - paragraph 21 – Purpose: occupational pensions (Related to article 9(2)(g))

Criminal conviction data:

Criminal conviction data requires conditions under both Article 6, and Article 10 of the GDPR to be met. Where we process information relating to criminal convictions, we rely on Schedule 1 Part 1 of the DPA 18: Paragraph 1 – Purpose: the processing for employment purposes.

As required by Schedule 1 of the DPA 18, Part4, we have an appropriate policy document in place relating to the safeguarding of processing under Schedule 1. This is available to all employees on the V drive.

If you fail to provide certain information when requested, this may affect your ability to perform your role in certain circumstances and/or we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

5. What is 'automated decision-making' and does EFL Trust use it?

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

6. Is my personal information shared with other organisations?

On occasion, we share your data with other organisations in their capacity as data controllers, and will put in place an appropriate data sharing agreement for such sharing. The organisations or categories of organisations are listed below:

- Other entities in the EFL Trust group (EFL, EFL Digital, and LFE), as EFL procure and provide a range of services to the EFL Trust, and EFL Trust carry out various charitable undertakings on behalf of the EFL. We would share your information in this way as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data, and in the day to day running of the business as relevant to your role.
- Pension providers (currently carried out through Broadstone and/or Standard Life);
- Organisations that provide work related benefits (such as Westfield and Vitality)
- Occupational Health/ other health providers
- External auditors (where this is necessary to carry out the audit)
- Government agencies (such as HMRC for tax purposes)
- Football clubs and/or community club organisations (where this is related to your work with those organisations, e.g. your contact details and job title).
- Football authorities (FA, PL, PLCF, PFA, LMA, NL) (where this is related to your work with those organisations, e.g. your contact details and job title).
- Commercial partners of the EFL group or EFL Trust(where this is related to your work with those organisations, e.g. your contact details and job title).

We share your data with third parties who act as data processors on our behalf. Where we employ a data processor, a contract that meets the minimum terms of Article 28 of the GDPR will be in place, to protect the processing of such data. We require third party processors to respect the security of your data and to treat it in accordance with the law. Your information will be shared with the following categories of data processors:

- Payroll, pension, and work related benefits administration services (some of this information is processed by EFL on our behalf, and payroll is currently carried out through ADP);
- Expense administration services (currently carried out through Concur);
- IT and some HR services (including EFL Trust desktop currently provided through EFL and Elite IT, meeting room booking facilities via Matrix, and online training tools).

This list will be updated regularly.

We may also share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. We may also need to share your personal information with a regulator, Court, dispute resolution service or to otherwise comply with the law (or to law enforcement authorities where we may be legally permitted to do so).

7. Will my information be transferred outside the EEA?

We do not transfer your personal information outside the EEA routinely. If we do, you can expect a similar degree of protection in respect of your personal information, and we will meet the requirement of the GDPR for international transfers.

We are committed to protecting the security of your personal data, which we generally hold in secure data centres in the European Economic Area (EEA).

Some organisations to which we may disclose your personal information may be situated outside of the EEA. Whenever we transfer your personal data out of the EEA, we take reasonable steps to ensure that your information is still properly protected by ensuring at least one of the following safeguards is implemented:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission. See https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en for further details.
- Where we use certain service providers, we may use contractual provisions to ensure your information is properly protected. For example, certain contracts are approved by the European Commission and give personal data the same protection it has in Europe.
- Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between Europe and the US. See
- https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en, for further details.

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

8. Is my personal information held securely?

We have put in place measures to protect the security of your information. Details of these measures are available in our data protection policies and record of processing activities on the V drive.

Third party processors will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

9. How long is my personal information retained for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our Data Retention Guidelines. Certain information may be retained in accordance with statutory requirements, including for tax purposes.

The retention schedule for your data can be found in Appendix 1 of this document.

10. What are my rights in connection with my personal information?

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in relation to the processing of your personal data are listed below, however not all rights are absolute, and are only applicable in certain conditions:

- Right to be informed: This privacy notice is designed to ensure you are fully informed about how we will process your data. Where we collect your information for a specific purpose in future (such as a staff survey), we will provide further, specific information to ensure this right is exercised.
- Right of access: (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it. You can exercise the right of access by contacting the DPO.
- Right to request correction (also known as rectification): This enables you to have any incomplete or inaccurate data about you corrected. If we cannot correct the

information for technical reasons, we will append a supplementary statement to the information.

- Request deletion (also known as right of erasure, or right to be forgotten): This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- Object to processing: this applies where we are relying on a legitimate interest (or those of a third party) and you want to object to processing on this ground. This also applies where we are processing your personal information for direct marketing purposes (and this right is absolute in relation to direct marketing – there are no further criteria required in this instance).
- Request the restriction of processing: You can ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or reason for processing.
- Request the data is transferred electronically (also known as the right to data portability): You can ask us to transfer your personal information to yourself or another data controller in a structured, commonly used, and machine readable format, where this is technically feasible.
- Right to withdraw consent: In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time.

Please note some of the above rights apply only in certain circumstances and/or be subject to conditions. For further information or to exercise any of these rights, please contact our Data Protection Officer.

You will not usually have to pay a fee to exercise these rights. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive (or refuse to comply with the request in such circumstances).

For security reasons we may need to request information from you to help us verify your entitlement to exercise any of your rights and/or to ensure that personal information is not disclosed to any person who has no right to receive it.

More information about where these rights apply can be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

11. Who can I speak to about my personal information held by EFL Trust?

We have appointed a Data Protection Officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO. You can e-mail your questions to info@efltrust.com.

You also have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

12. Will this policy change?

We may update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

APPENDIX 1 – Retention Schedule

Information processed for:	How long will we keep this information?
Information relating to the recruitment process, (references, application form, CV or cover letter).	6 months for unsuccessful candidates. For successful candidates this will be kept in your personnel file as retained as below.
Information relating to your employment, in order for us to perform HR processes, such as your personnel file.	7 years following the end of your employment with EFL Trust.
Payroll and expenses information.	7 years following the end of the financial year.
Annual leave	7 years
Maternity, paternity, adoption, and sick leave	7 years following the end of the next financial year.
Performance information, such as training and development records.	7 years following the end of your employment with EFL Trust.
Information about your salary and work-related benefits.	7 years following the end of your employment.
Monitoring Information (such as swipe cards and CCTV).	1 month following use (unless otherwise required by law).
Equal opportunities monitoring.	Anonymised after 6 months.

Copy of any contracts.	7 years after contract end.
Emergency contact details.	End of employment.
Criminal records checks (DBS)	Criminal records information not retained. DBS physical form returned to data subject immediately.

At the expiry of the relevant retention period, information will be reviewed to assess whether it can be destroyed or whether retention is required for a further period.