Data Protection Policy
May 2018

V1.0

The FA's Data Protection Policy

1. PURPOSE

This document sets out The FA's commitments and obligations when it processes personal data about individuals. It also sets out The FA's basic expectations of The FA's employees, workers and supplier staff when they handle personal data.

References throughout this policy to The FA, we or us are to The Football Association Limited and all its subsidiary companies from time to time including, Wembley National Stadium Limited and The National Football Centre Limited.

Please ensure you read this document in full.

2. INTRODUCTION AND SCOPE

2.1 What is personal data and what is a data subject? What is sensitive personal data?

Personal data is any information held about an identifiable living individual – also known as a "data subject" - about which The FA processes personal data. An individual can be identifiable both where The FA holds clear direct identifiers about them or where The FA can identify the individual by other reasonable means, such as using other data held by The FA or which is publicly available.

Data protection rules give some examples of information that are direct identifiers, and must be considered personal data, such as name, an identification number, location data, and online identifiers such as IP address. Other examples include payment information, decisions made about individuals and even subject opinions they hold, or that are held about them.

Sensitive personal data is any information about health, religion, sex life or orientation, racial or ethnic origin, political opinions, trade union membership, genetic data or biometric data that can uniquely identify a person (such as fingerprints or facial recognition technology). Where this policy discusses sensitive data, it also includes information about criminal convictions, or alleged criminal activity, which is governed by very similar rules.

2.2 What is processing?

Processing is any use that The FA – or a third party - makes of personal data, whether for itself or for a third party. This includes creating data, amending it, storing it, sharing it, or even accessing, anonymising or deleting it.

2.3 What obligations does The FA have?

Where The FA chooses what data will be processed and for what purposes, it is a data controller and in charge of ensuring that all data protection requirements are met. For

example, The FA is a data controller for the information held about its employees, and as governing body for the personal data it uses in carrying out its regulatory, disciplinary and organisational functions in football and as providers of goods and services in relation to its competitions, tickets and tours.

Where it processes personal data only as a service on behalf of other data controllers and under their instructions, with no independent use for that data, The FA is a processor of that personal data. For example, The FA is a processor where it provides software services to others in football where it has no independent use of the data, such as where it provides FullTime to leagues.

The FA may act as a data controller or as a data processor for different activities – including different uses of data on the same system. If you are in any doubt as to whether The FA is a data controller or a data processor for a particular function you are involved in, you can contact The FA's Legal team for clarification by emailing dataprotection@thefa.com.

Both data controllers and data processors have obligations under the General Data Protection Regulation (or "GDPR") and under applicable local laws such as the Data Protection Act 2018 and Privacy & Electronic Communications Regulations 2003. The FA's obligations under these laws are summarised in this policy.

2.4 What are my obligations?

All workers and suppliers of The FA must assist it in complying with this Data Protection Policy and have a duty to respect the commitments, procedures and practices set forth in this Policy and any associated policies. This Policy is also a part of The FA's Employee Handbook and failure to comply with this Policy may result in disciplinary action.

This is The FA's main Data Protection Policy. There may be, for your department or function, or for specific systems you use, specific guidance or training materials that set out in greater detail how you can best help The FA comply with applicable data protection rules. There are also more detailed FA policies in respect of data subject rights and personal data incident notification which can be found on TeamTalk.

3. CORE DATA PROTECTION PRINCIPLES

The FA observes the following data protection principles when processing personal data:

3.1 Lawfulness, Fairness and Transparency

Fairness and legal basis

Where The FA acts as a data controller, it may only process personal data fairly and lawfully and in particular it must have a legal basis for processing personal data. Examples of a relevant legal basis for processing include:

a) the processing is necessary for the performance of a contract with the data subject, or in order to take steps at the request of the data subject prior to entering into a contract;

b) the processing is necessary for compliance with a legal obligation to which The FA is subject;

c) the data subject has given consent; or

d) the processing is necessary for the purposes of the legitimate interests pursued by The FA – or a third party - except where these interests are overridden by the interests or fundamental rights and freedoms of the data subject. The FA will need to carry out a balancing test to ensure that its legitimate interests justify the intrusion and outweigh any contrary interests of the data subject. Examples of specific circumstances where The FA has carried out a balancing test are set out in Annex 1 to this Policy.

Where The FA needs to process sensitive personal data as a data controller, it must also have an *additional* legal basis on which to process data, to overcome the general ban on processing such information. Relevant legal grounds can include compliance with employment laws, preventing and detecting unlawful activity, the explicit consent of the data subject or specific grounds for processing data to safeguard individuals at risk, carry out anti-doping measures or measures necessary to protect the integrity of football where this is in the substantial public interest.

Legal will be able to provide further information on the relevant legal basis for a particular activity or function if you need further assistance.

Fairness and Transparency

When The FA collects personal data from data subjects, it must inform them of:

a) the identity and the contact details for The FA – or the relevant FA company which is the data controller;

b) the contact details of The FA's Data Protection Officer;

c) the purposes and the legal basis for the processing;

d) the legitimate interests of The FA, where applicable;

e) the recipients or categories of recipients of the personal data;

f) any international data transfers, including the location of any recipients and the methods used to ensure the adequate protection of those transfers (and how to obtain details of those methods);

g) data retention periods;

h) their rights under data protection rules;

i) the process available to data subjects to withdraw any consent;

j) whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such data; and

k) the existence of automated decision-making, including profiling, and the logic involved.

When The FA acts as a data controller for personal data collected from any other source, or creates the data itself, it must additionally inform the data subject about the source of the personal data. This information must be as precise as possible.

The FA must provide this information at the time it collects the data from the data subject, or if it collects the data from another source, it should provide this information within a reasonable period, being no later than one month after the data was obtained or created by The FA. If The FA intends to communicate with the data subject, or disclose the data to a third party, then information must be provided no later than that communication or disclosure.

Privacy policies must be provided in a concise, transparent, intelligible and easily accessible way, using clear and plain language (in particular where the data subject is a child). Where the provision of information proves impossible or would involve a disproportionate effort and data is not being obtained directly from the data subject, The FA may be permitted to instead include details of the processing in a public facing policy. This must be approved by FA Legal – and it may require the completion of a Data Protection Impact Assessment.

In exceptional circumstances, and only with the approval of FA Legal, the provision of specific information may be postponed or omitted, for example, in the context of investigations into wrongful conduct or to comply with applicable laws or where provision of the information could jeopardise the integrity of an investigation. The FA should still provide general information in relation to this type of processing wherever possible – for example, The FA provides general information about the type of processing it carries out in relation to investigating corruption and integrity matters in its publicly available Participant Privacy Policy, and this is brought to the attention of participants.

The FA's main privacy policies for its fans and participants can be found on The FA's website: a list of the main policies is included at the bottom of the main FA website privacy policy. The FA's privacy policies for staff can be found on TeamTalk. Where a privacy policy is not provided online, a copy of this can be requested from FA Legal/the DPO.

Where carrying out any new processing, or making a change to any existing processing, you should check that this does not require a change to any FA privacy policy. If you are trying to identify the relevant privacy policy for your function, you should contact your team's GDPR Champion or FA Legal.

If any new processing or changed processing is not covered by an FA privacy policy, you must discuss this with FA Legal prior to carrying out this new activity. FA Legal will help you check whether the change is necessary, and whether there is a need to update or provide a new privacy policy to data subjects. Information in respect of any new or changed processing must also be included in the ITT, Project Charter or Change Request which is completed in respect of the project.

3.2 Purpose Limitation and Data Minimisation

The FA must only process personal data for the purposes for which it was originally collected. The FA cannot use personal data in a manner that is incompatible with the original purpose unless an exception is provided under law or a new consent has been obtained from the data subject.

In any case, you should consult FA Legal where you or your team intend to process personal data for a new purpose so that they can help you assess necessity and compatibility and ensure that The FA can meet other obligations in respect of privacy policies.

The FA shall only process adequate, relevant and limited personal data of data subjects, ensuring that only data that is necessary for the specified purposes is processed and retained by The FA. The FA has put in place appropriate measures to ensure privacy by design and by default. These are discussed in more detail in the "Accountability" section below.

3.3 Accuracy

The FA must ensure that information is accurately recorded and kept up to date. Individuals also have a right to correct information that The FA holds about them. Where this is objective information, The FA takes steps to ensure that its methods of collecting data (both directly and indirectly) ensure that data is accurate (for example, by providing clear collection forms, taking steps to automate data collection to reduce transcription errors and putting in place systems to reduce duplication). Individuals must be given opportunities to view and update their information where possible. Where information is subjective, and The FA does not agree with the change, The FA must be able to annotate and record the data subject's views and disagreement.

You should take particular care to ensure that data is recorded accurately, and ensure that you respond promptly where a request is received to update or correct information. If there is any concern that the request to correct information may be inappropriate, you should escalate the request in accordance with The FA's Data Subject Rights Policy.

3.4 Storage Limitation

The FA must keep personal data in an identifiable form for no longer than is necessary for the purposes that The FA has collected and processed it. Specific details in respect of the retention periods that The FA has adopted for its different purposes and processing activities are set out in The FA's privacy policies and records of processing.

The FA subjects these retention policies to regular review: specific examples of how often these are reviewed for high risk data are set out in the Data Protection Impact Assessments carried out for high risk processing and, for processing of other sensitive data not requiring a Data Protection Impact Assessment, in Annex 2 to this policy.

Where a retention period is reached, The FA is committed to taking appropriate action to ensure that the relevant data is no longer processed by The FA in an identifiable form. This may involve deleting the data, returning it to the data subject or elected third party, or anonymising the data, depending on what is most appropriate in the circumstances.

You should ensure that you abide by the retention periods set out in the record of processing, and particularly ensure that any obligations on you or your department to keep retention under review are followed. If you no longer require data, you should make sure this is appropriately disposed of or anonymised – you should reach out to FA Legal if you have any questions over how to best dispose of data or ensure that it is anonymised.

3.5 Integrity and Confidentiality

The FA may only collect, process and disclose personal data in a manner that ensures appropriate security of that personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The FA has a number of policies that address the need to keep personal data secure – please see the Information Security Policy and the Everyday Security Policy for more details. You must ensure that you follow all relevant security policies, and take the steps set out in those policies to keep data secure.

The FA is also required to ensure that it has a robust data breach response program in place, so that it can log, remediate and report any personal data breaches as required by law. The Personal Data Incident Management Policy provides more information on what constitutes a data incident and your responsibilities for reporting and managing such an incident. This policy can be found on TeamTalk. You should ensure that you follow this policy, and ensure that any suspected or actual data incidents or breaches of any of the security policies which involve personal data are reported to the IT Service Desk on extension 4555, 0800 902 0014, itsupport@thefa.com as soon as you become aware of the incident.

Where The FA deals with third parties, it may need to enter into written agreements with those third parties to ensure that any personal data which is shared as part of that relationship is appropriately protected – whether that third party is a data controller or a data processor. If you intend to enter into a relationship with a third party that will involve the exchange of personal data, please contact FA Legal to ensure that appropriate contracts and arrangements are put in place. For further information about data sharing, please see the data sharing section below.

3.6 Accountability and Data Governance

The FA must be able to demonstrate compliance with the principles set out above. The processes and procedures adopted by The FA to ensure and document compliance include the following:

- Privacy by design and default: When acting as a data controller, The FA has adopted appropriate risk assessment procedures to ensure that appropriate technical and organisational measures are adopted to protect personal data and that these have been appropriately included in The FA's processing activities, products and services.

- Data Protection Impact Assessments: When acting as data controller, The FA will carry out data protection impact assessments on any "high risk" processing activity before it is commenced. Such assessments will include a description of the processing activities and their purpose and an assessment of the need for and proportionality of the processing, the risks arising and measures adopted to mitigate those risks, in particular any safeguards and security measures which are needed to protect personal data and comply with the law. The need to carry out a new data protection impact assessment, or review an existing impact assessment, will be identified through the privacy by design process. This process will be managed jointly by FA Legal and IT, and all impact assessments will be reviewed by the DPO to confirm whether risks have been appropriately mitigated.

- Data Protection Officer ("DPO"): The FA has appointed a DPO, Richard McDermott. The DPO acts as the primary contact for relevant data protection authorities such as the Information Commissioner's Office and has (amongst others), the following duties: to inform and advise The FA and it employees of their obligations under the applicable privacy legislation and to ensure compliance with those laws; to monitor compliance with privacy legislation and with related policies of The FA; and to provide advice to The FA where requested on data protection impact assessments and their implementation.

- Records of processing: The FA keeps a record of any processing of personal data (including the type of personal data processed, the relevant data subject and the purposes for which it is used) which it carries out both as a data controller and as a data processor. These records of processing are reviewed whenever existing

processing is changed or new processing takes place, and any relevant updates are made. Major updates are made on an ad-hoc basis where required. The updating process is led by the GDPR Champions, with support from FA Legal where needed. Wherever you are aware of a change to data processing carried out by you or your team, you should ensure that your GDPR Champion is notified so that an update can be made to the record of processing. GDPR Champions can seek further advice from FA Legal as required.

3.7 Data Processor principles

The requirements in this section 2.7 apply exclusively where The FA processes personal data as a data processor on behalf of a third party under a data processing agreement. Examples of The FA's activities as a data processor include its provision of certain software solutions to County FAs or to other football stakeholders. In general, where The FA acts as a data processor, it will, to the extent reasonably possible, co-operate and assist the relevant data controller to comply with its obligations under applicable law.

Where The FA acts as a data processor and processes personal data on behalf of a third party data controller, it shall comply with the data processing commitments set forth in the relevant data processing agreement. It shall promptly notify the data controller if, in its opinion, any instruction received from the data controller is contrary to applicable data protection laws.

Specific duties on The FA where it is a data processor include:

3.7.1 Purpose limitation

The FA will only process personal data it receives as a data processor for the purposes set out in the data controller's instructions as contained in the data processing agreement, as otherwise given to The FA in writing or as otherwise required by law.

Where obliged to process such personal data for other purposes by law, The FA will inform the data controller before such processing, unless such law restricts its ability to notify on important grounds of public interest.

3.7.2 Data integrity

At the end of The FA's provision of the data processing services to the data controller, The FA will, at the choice of the data controller, return or destroy all relevant personal data and copies of that personal data and certify that this has been done, unless law requires storage of the personal data. Where such restrictions apply, The FA will inform the data controller and warrant that they will guarantee the confidentiality of any personal data retained or transferred, and not actively process it any further unless required by that law.

The FA will implement any measures required by the data controller in order to ensure that personal data is updated, corrected or deleted. The FA will also ensure that any other third parties involved in the data processing that have received relevant personal data are aware of any request to rectify or delete such personal data. The FA will execute any necessary measures, when asked by the data controller, in order to have the data deleted or anonymised from the moment the identification form is no longer necessary. The FA will communicate the deletion or anonymisation of the personal data to all other relevant third parties or data processors that have received the personal data.

3.7.3 Security

The FA will, at a minimum, comply with its obligations under Article 30 of GDPR and any security and organisational requirements required by the law applicable to the data controller and any measures specified in the data processing agreement. The FA will inform the data controller of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data without undue delay, and in accordance with any policy set out in the data processing agreement or by The FA's own data breach response program.

3.7.4 Individual rights

The FA will to the extent possible and taking into account the nature of the processing, assist the data controller by appropriate technical and organisational measures, so that the data controller can comply with its obligations in relation to individual rights under applicable law. The FA will also communicate any useful information in order to help the data controller comply with such obligations. The FA will forward any request received from an individual where it only holds their data as a data processor to the relevant data controller without answering it unless The FA is authorised by the data controller to act on requests on its behalf.

3.7.5 Sub-processors

The FA will only use third party subcontractors to process the personal data as a sub-processor where:

(a) Appropriate prior information has been given to the data controller (including information on the main elements of the processing (for example, the name of the relevant entity, where they are located, security measures, and guarantees in case of international transfers)).

(b) The prior consent of the data controller has been obtained. The relevant agreement with the data controller must state if a general prior consent is given to the use of new sub-processors or if specific consent will be required for each new sub-processing. In any case where a general consent is given, The FA will inform the data

controller of any intended changes concerning the addition or replacement of any sub-processors in a timely fashion.

(c) The FA will put in place a written agreement with the relevant sub-processor which contains the same requirements as apply to The FA under the data processing agreement, and will remain fully liable for the sub-processor's performance of its data processing obligations.

4. DATA SUBJECT RIGHTS

Data subjects can exercise their rights under the law at any time by contacting The FA using the contact details set out in the relevant privacy policies, or by contacting the DPO. Data subjects are entitled to use other means to means to make requests to The FA, provided that they are received by The FA in writing. All requests from data subjects will be processed in compliance with The FA's Data Subject Rights Policy. You should ensure that you are aware of the processes set out within The FA's Data Subject Rights Policy, so that you can recognise a request made by a data subject and escalate it immediately in accordance with that Policy. The rights available to data subjects which you must be able to recognise are as follows:

- Rights of access and portability: The FA must, on request from a data subject: (i) confirm if The FA processes relevant personal data; (ii) provide a copy of the personal data (in a commonly used electronic form in many cases); and (iii) provide supporting explanatory materials. For personal data provided by the data subject which is processed automatically, and which The FA processes with the individual's consent or to fulfil a contract with that individual, The FA must transfer (or "port") the relevant personal data to a new service provider if so requested, or make the relevant personal data available to the individual, in machine readable and structured format. Relevant exemptions may exist to such disclosures, particularly where disclosures would adversely affect the rights and freedoms of others.

- Right of rectification: The FA will consider and, where required, comply with requests from data subjects to rectify inaccurate personal data. The FA must only process accurate personal data and must ensure that personal data is kept up-to-date. If a data subject submits a valid claim that the personal data The FA maintains about them is incorrect, The FA must work to rectify the inaccuracy. Where The FA is a data processor, it will implement any security measures required by the data controller in order to ensure that personal data is kept accurate and up-to-date in accordance with section 2.7.4 above.

- Right of objection: The FA will consider and, where required, comply with requests from data subjects who object to: (i) direct marketing; (ii) scientific, historical or statistical research; and/or (iii) processing justified based on legitimate interests.

- Right of erasure (the "right to be forgotten"): The FA will consider and, where required, comply with requests from data subjects for their personal data to be "erased". The FA must comply with such requests when there is a problem with the underlying legality of the processing or where the processing was based on consent and this consent has been withdrawn, or where the data subject has validly exercised a right to object and wishes the data to be erased.

- Right of restriction: The FA will consider and, where required, comply with requests from data subjects to "restrict" the processing of personal data whilst complaints (for example, about accuracy) are resolved, or if the processing is unlawful but the data subject objects to erasure.

- Automated decision-taking: The FA will not take decisions based solely on the automated processing (i.e. with no human involvement) of a data subject's personal data which produce legal effects, or have similarly significant effects unless permitted by law and after consulting with FA Legal to ensure appropriate safeguards are put in place.

5. SHARING DATA WITH THIRD PARTIES AND INTERNATIONAL TRANSFERS

Any third party appointed to collect, store or use personal data as The FA's data processor must provide satisfactory assurances and contractual commitments as required by applicable law. Third parties acting as data processors will be subject to a data protection and information security risk assessment before they start providing any service. Third parties who act as The FA's data processor must enter into a written agreement with The FA which ensures that it will provide adequate privacy, data protection and information security measures. Such agreements shall include, at a minimum, certain contractual safeguards, including clear details on what data the third party is processing on The FA's behalf and what processing service they are providing. You should ensure you follow the standard FA procurement process, speak to the Procurement Team and use the standard Invitation to Tender template which requests data protection and information security policies from potential suppliers.

Where The FA transfers personal data from data subjects to third parties acting as data processors that are (i) located in countries that do not provide adequate levels of protection(ii) not covered by approved binding corporate rules; or (iii) who do not have other arrangements that would satisfy EU adequacy requirements, The FA has to ensure that appropriate contractual controls, such as model contractual clauses approved by the European Commission are implemented unless an appropriate exemption exists.

When The FA, acting as a data controller, shares personal data with third parties that are also data controllers, The FA will ensure that there is a legal basis under the applicable law for such data sharing and will implement appropriate measures to address any relevant data transfers outside the EU to such third parties unless an appropriate exemption exists.

You should contact FA Legal where you believe that will be a new transfer outside the EU or a change to an existing transfer, so that they can assist you in identifying and putting in place an appropriate transfer mechanism.

6. TRAINING

The FA shall provide training on this and The FA's other data protection policies and obligations to all employees and workers who collect, use or have access to or responsibilities associated with managing personal data, or who are involved in the development of products, services or tools used to process personal data. In particular, The FA provides compulsory online training to all staff, and requires GDPR Champions to have specific training on FA policies. The FA also provides additional training and guidance to teams that handle particularly complex data or require specific assistance with complying with data protection obligations.

7. AUDITS AND MONITORING

The FA will perform audits of compliance with this policy and other data protection policies. The Audit Committee may also choose to audit on-going GDPR compliance including compliance with this policy.

The FA will ensure that any issues or instances of non-compliance with this policy identified by audits or otherwise are brought to the attention of the DPO, FA Legal and HR as required, and that appropriate corrective actions are taken to ensure compliance.

8. UPDATES OF THE POLICY

FA Legal is responsible for communicating changes to this policy to FA employees.

ANNEX 1: FA balancing tests for legitimate interests processing

The FA carries out a number of activities on the basis of its legitimate interests. It will only process any personal data on the basis of legitimate interests where it is confident that it (a) has identified a legitimate purpose for the processing; (b) considers the processing to be necessary to achieve that purpose and (c) has considered the data subject's interests, and believes that, given that nature of the data, the reasonable expectations of the data subject and the likely impact on the data subject – together with any safeguards that can be put in place – the processing is justified.

Wherever The FA carries out processing based on its legitimate interests, individuals are able to exercise a right to object. The FA will carefully consider any such request, and in particular whether its own interests – or those of others – are compelling, and require the on-going processing of that data.

Processing that The FA carries out on the basis of its legitimate interests include the activities set out below. Balancing tests may also be set out in privacy policies, department specific guidance or in Data Protection Impact Assessments.

Marketing	
The FA has confirmed that its processing for these purposes is not speculative, and that the intended processing is compliant with The FA's security policies and privacy by design principles.	
Purpose test	The FA wants to be able to promote its products, services and values, including through marketing communications. In the case of certain marketing (particularly to Club Wembley members) marketing is done on the basis of legitimate interests. The FA uses contact details obtained from its business and consumer contacts in order to send marketing about its products and services by post and to make marketing calls. Where The FA has obtained information about a consumer directly from that consumer as part of the negotiation or sale of a service, it may also contact that consumer by email about similar products or services where they have been given the opportunity to opt out at the outset. It may also send marketing emails to business contacts that are not subject to the ePrivacy legislation.
Necessity test	The FA only conducts marketing and promotion in a manner described in its privacy policies, and ensures that it only carries out such marketing in a proportionate manner. It follows a clear marketing strategy internally, and is careful to deliver or communicate a reasonable level of promotional material to its contacts.
Balancing test	The activity is reasonably foreseeable and mentioned in relevant polices. Individuals are able to opt out at any time, including from the message

	when contacted by email. The FA makes appropriate use of the Telephone Preference Service to ensure that any phone marketing complies with relevant laws. Retention limits are put in place to ensure that disengaged contacts are removed from marketing lists even if no opt out is received. **Threat to The FA if processing could not take place:** medium, as an inability to promote and advertise certain products/services could have a substantial commercial impact. **Threat to individuals (taking into account mitigation):** limited, as individuals have a clear right to object that can be readily exercised at any relevant opportunity.

Fraud monitoring	
The FA has confirmed that its processing for these purposes is not speculative, and that the intended processing is compliant with The FA's security policies and privacy by design principles.	
Purpose test	Where The FA enters into contracts with data subjects, it will also carry out necessary fraud monitoring to ensure that it is dealing with verified individuals and legitimate payment methods and delivery addresses are being used. This purpose is recognised in the GDPR as a legitimate interest, and helps to protect both The FA and individuals from the fraudulent activities of others.
Necessity test	The FA ensures that it only carries out fraud monitoring where this is necessary in relation to the product or service being offered to a data subject, and that checks are carried out at the latest possible time.
Balancing test	Although the processing may disclose wrongdoing, it would do so to the benefit of an individual or company (including The FA) that is being defrauded. The processing helps prevent and deter unlawful activity, and allows The FA to continue dealing with other individuals over the internet. The activity is reasonably foreseeable and mentioned in relevant policies. **Threat to The FA if processing could not take place:** high, as failure to process data could lead to individuals and The FA being put at risk of fraud. **Threat to individuals (taking into account mitigation):** limited, unless they are involved in wrongdoing. Individuals are appropriately warned about the processing and only issues that suggest fraud may be taking place will be flagged and reviewed.

Network and Information Security	
The FA has confirmed that its processing for these purposes is not speculative, and that the intended processing is compliant with The FA's security policies and privacy by design principles.	
Purpose test	The FA uses relevant monitoring tools on both its internal and external facing systems, sites and applications, and on its infrastructure, to ensure that it can prevent an detect any unlawful or prohibited activity, including breaches of data security measures adopted to comply with the GDPR and applicable data protection laws. This purpose is recognised in the GDPR as a legitimate interest, and helps to protect both The FA and the personal data of data subjects The FA processes on its systems, sites and applications
Necessity test	The FA ensures that it uses appropriate monitoring solutions, and only investigates the activities of specific individuals where a solution has flagged suspicious activity. Access to the data involved in this purpose is limited to appropriate information security personnel unless the monitoring indicates wrongdoing that must be reported to HR or to law enforcement personnel.
Balancing test	Although the processing may disclose wrongdoing, it would do so to the benefit of individuals whose data may be put at risk and/or the commercial interests of The FA or its partners. The processing helps prevent and deter unlawful activity and to reinforce security measures adopted to comply with GDPR and applicable data protection laws. The activity is reasonably foreseeable and mentioned in relevant policies. Specific investigations into the activity of an employee are only carried out where there is a relevant suspicion, and with the approval of the appropriate leadership within HR and IT. **Threat to The FA if processing could not take place:** high, as failure to process data could lead to wider information and security risks for The FA, due to the inability to use appropriate tools to monitor threats to its systems and software. **Threat to individuals (taking into account mitigation):** limited, unless they are involved in wrongdoing. Individuals are appropriately warned about the processing and only behaviour that creates a suspicion of wrongdoing will be flagged and reviewed.

ANNEX 2: Examples of how The FA deals with data retention

The FA adopts appropriate retention periods for its processing of personal data, to ensure that data is only held as long as is necessary for its identified purposes. Personal data that is retained at the point of a retention limit being met is taken out of active use, and is then held for a limited three month period to ensure that any links to that information across other FA systems is not degraded over that period. At the end of this period, the data is fully deleted, transferred to the data subject or transferred to an appropriate third party or anonymised at the point a limit is reached.

In some limited circumstances, it is not appropriate or possible to set a firm period at which data will be removed – this is due to a need to make a case by case assessment about whether information held is still necessary for the relevant identified purposes. In these circumstances, The FA has identified regular intervals at which data will be manually reviewed by the appropriate business team, and an ongoing need to retain the data identified.

A full list of retention periods can be found in the relevant record of processing held by The FA – details of relevant periods are also communicated to individuals in appropriate privacy policies.