

CRICKET REGULATOR GUIDELINES ON THE SURRENDER OF ELECTRONIC DEVICES

1. Introduction

- 1.1 The Cricket Regulator is the body responsible for monitoring compliance with the cricket regulations set by the England and Wales Cricket Board Limited (**ECB**), and for the enforcement of adherence to those regulations. This includes the ECB's [Disciplinary Procedure Regulations](#) (**DPRs**). The Cricket Regulator was established in December 2023 and is overseen by the independent Cricket Regulatory Board. The Cricket Regulator sits within the ECB, but it acts independently of the ECB in relation to the conduct of cases and has separate reporting lines.
- 1.2 These guidelines explain how the Cricket Regulator may exercise its power under the DPRs to request that you (as a Participant) surrender your Electronic Devices (defined below) to the Cricket Regulator for forensic analysis as part of an investigation into an alleged or suspected breach of the Applicable Regulations (defined below).
- 1.3 For the purpose of these guidelines, the following terms have the following meanings:
- 1.3.1 **"Applicable Regulations"** means the ECB rules and/or regulations (or any successor rules or regulations) as set out in Regulation 1 (Definitions) of the DPRs.
 - 1.3.2 **"Application"** means the internal application prepared by the Cricket Regulator investigator for a Demand.
 - 1.3.3 **"Charge"** means a charge brought by the Cricket Regulator against a Participant in respect of an alleged breach (or breaches) of the Applicable Regulations.
 - 1.3.4 **"Demand"** means a written demand, in the standard form issued by the Cricket Regulator from time to time, requesting access to an Electronic Device (or Electronic Devices) as set out in Regulation 3.5 of the DPRs.
 - 1.3.5 **"Electronic Device"** means any portable device (including, without limitation, a mobile phone, tablet, or smartwatch) which is capable of connecting to or using any wired, wireless or mobile telecommunications technology to enable or facilitate transmission of text based material, data, voice, video or multimedia services, and any device which stores electronic information (including, without limitation computers and/or hard drives).
 - 1.3.6 **"Encrypted Device"** means the encrypted digital intelligence platform used by the Investigators to review the data extracted from the Electronic Device, such as a UFED.
 - 1.3.7 **"Investigator"** means the Cricket Regulator member of staff investigating an alleged or suspected breach of the Applicable Regulations.
 - 1.3.8 **"Participants"** means any individual or entity listed in Regulation 2.1 of the DPRs (and these guidelines may refer to a relevant Participant subject to a Demand as **"you"** or **"your"**).

1.3.9 "UFED" means the Universal Forensic Extraction Device.

2. Surrender of Electronic Devices

- 2.1 The Cricket Regulator is committed to removing, disrupting and countering the full range of misconduct which impacts cricket, including discrimination, sexual misconduct, financial misconduct, and corruption. In the modern age, these serious types of misconduct are often being conducted online and facilitated through the use of Electronic Devices. Electronic Devices are therefore a key source of evidence for an investigation, as they often contain relevant communications, records, and data that can help Investigators establish the facts of an alleged or suspected breach of the Applicable Regulations.
- 2.2 Under Regulation 3 of the DPRs, the Cricket Regulator has the power to conduct investigations into alleged or potential breaches of the Applicable Regulations. The Cricket Regulator has a number of investigatory powers to enable this process, which includes the ability to issue a Demand to Participants to provide access to their Electronic Devices. In order to exercise this power fairly and proportionately, the Cricket Regulator only intends to use this power to issue a Demand if:
- 2.2.1 it has reasonable grounds to believe that a Participant has committed a breach of the Applicable Regulations, and it is not possible to gather evidence of the breach through other investigative means;
 - 2.2.2 the Cricket Regulator considers that the nature and seriousness of the alleged breach meets the required threshold. This will include investigations into allegations of sexual misconduct and serious safeguarding concerns, corruption or serious financial misconduct, supplying prohibited substances or attempts to evade testing anti-doping protocols, or organised or systemic discrimination;
 - 2.2.3 it is reasonably likely that the surrender and analysis of the Electronic Device will assist the investigation because there is a reasonable suspicion that the Electronic Device contains evidence relevant to the investigation; and
 - 2.2.4 the decision to issue a Demand has been approved by the Managing Director of the Cricket Regulator (or the Deputy Director of the Cricket Regulator in the event that the Managing Director is unavailable to authorise the Demand).
- 2.3 When issued with a Demand, you are required to:
- 2.3.1 provide the Cricket Regulator with your Electronic Device and provide access to any social media accounts and cloud storage (including your usernames and passwords) within a timeframe set out in the Demand. This could include a request for the immediate provision of the Electronic Device; and
 - 2.3.2 allow the Cricket Regulator (and its third-party forensic partner) to copy, download, extract and obtain information from the Electronic Device, namely any data, messages, photographs, videos, audio files, documents or other relevant material (as further described in paragraph 5.2 below) contained on the Electronic Device which are relevant to the investigation.

2.4 Compliance with a Demand is voluntary. You may refuse to consent to the surrender of your Electronic Device in accordance with the Demand, or you may agree to comply with the Demand in part or on certain conditions. In such circumstances, you will be asked to set out your reasons in writing for refusing to comply with the Demand (in whole or in part), and the Cricket Regulator will consider whether these explanations are reasonable and justified. If the Cricket Regulator concludes that you have unreasonably or unjustifiably refused to cooperate with a Demand:

2.4.1 an adverse inference in relation to the non-compliance may be drawn by the Disciplinary Tribunal and/or Appeal Panel (if applicable) as part of any disciplinary proceedings relating to the offence which is being investigated by the Investigators (in accordance with Regulation 8.19.4 of the DPRs); and/or

2.4.2 you may be charged with a separate offence of failing to cooperate with an investigation (in accordance with Regulation 3.9 of the DPRs).

3. The Process for Authorising a Demand

3.1 When undertaking an investigation into an alleged or suspected breach of the Applicable Regulations, the Investigator will make an initial assessment as to whether a Demand should be issued to a Participant. This assessment will be based on the evidence currently available to the Investigator, and the factors set out in paragraph 2.2 above.

3.2 If the Investigator concludes that the Demand should be issued to a Participant, the Investigator will complete an Application and submit it to the Cricket Regulator's Head of Investigations for review and approval. If the Head of Investigations determines that the information provided in the Application is not sufficient to issue a Demand, the Application will be refused and returned to the Investigator.

3.3 If the Head of Investigations determines that the Application is sufficient to issue a Demand, the Head of Investigations will submit the Application to the Managing Director of the Cricket Regulator for final approval. If the Managing Director authorises the Application, the Cricket Regulator will prepare the Demand. The Demand will set out the details of the request, including the Electronic Device required (or Electronic Devices, noting that one Application and Demand can apply to multiple Electronic Devices so long as they are provided in respect of the same Participant), the information required to access the Electronic Device, and the process for extracting data from it. The Cricket Regulator will then serve the Demand on the relevant Participant following the process set out in section 4 below.

3.4 The Cricket Regulator may request that "non-suspect" Participants, such as victims and witnesses, voluntarily share relevant material held on their Electronic Device which support their testimony or otherwise assist the investigation. However, the Cricket Regulator does not intend to issue a Demand under Regulation 3.5 of the DPRs to "non-suspect" Participants routinely or as a matter of course, and instead reserves the right to do so only in:

3.4.1 circumstances where the "non-suspect" Participants have refused to share relevant materials with Investigators upon the Investigators' informal request; and

- 3.4.2 the most exceptional and serious cases where the Investigators deem it necessary to assist the investigation.

4. Process for Issuing a Demand

- 4.1 Once the Demand has been authorised in accordance with the process outlined in section 3 above, the Investigators will serve the Demand on the Participant. This will normally be done in person and without prior notice. Once a Participant has received a Demand, there are three potential outcomes:

4.1.1 The Participant agrees to comply with the Demand. In such circumstances, the Participants will be required to sign a consent form, and the Investigators will take possession of the Electronic Device for data extraction and analysis. This process is outlined further in paragraphs 4.2 and 4.3 below.

4.1.2 The Participant requests time to take legal advice. In such circumstances, the Investigators will take possession of the Electronic Device and store it securely in a tamper-evident bag. This is to prevent the Participant from tampering with the Electronic Device while they seek and receive legal advice. However, the Investigators will not use or extract any information from the Electronic Device until the Participant provides their consent for this. If the Participant consents, the process outlined in paragraph 4.1.1 (and below) will be followed. If the Participant refuses to consent after obtaining legal advice, the process outlined in paragraph 4.1.3 will be followed.

4.1.3 The Participant refuses to comply with the Demand. In this case, the Participant will retain access to their Electronic Device and be asked to provide a written explanation for refusing to comply with the Demand. The Participant will be told that if the Cricket Regulator determines that the refusal is unreasonable or unjustifiable, it may draw an adverse inference from the Participant's refusal to surrender their Electronic Device, which will be considered as part of the disciplinary process, and it may issue the Participant a separate charge for failing to cooperate (as outlined further in paragraph 2.4 above).

- 4.2 If the Participant provides their consent to Investigators as outlined in paragraph 4.1.1 above, the Investigators will take possession of the Electronic Device. If it is possible to undertake an "at venue" extraction of data from the Electronic Device, the Investigators and/or the third-party forensic partner will download and extract the relevant data from the Electronic Device at the same location where the Demand was issued as outlined in section 5 below, and once that process has been completed, the Electronic Device will be returned to the Participant.

- 4.3 If an "at venue" analysis and data extraction is not possible, the Electronic Device will be stored securely in a tamper-evident bag and taken away by the Investigators for data extraction. The Investigators will hand deliver the Electronic Devices to the third-party forensic partner to conduct the data extraction as outlined in section 5 below.

5. Use of Electronic Device and Data

- 5.1 To enable the data extraction process by the third-party forensic partner, the Investigators will identify and specify what data is to be targeted for extraction, and where possible the extraction will be limited to the data relevant to the investigation

only. For example, if the investigation concerns the communications between two known individuals, the data extraction will be limited to the messages and communications between those two individuals. However, in more complex cases, limited and targeted extraction may not be possible, in which case the third-party forensic partner will be instructed to download and extract all the data from the Electronic Device or to make a forensic image of the Electronic Device (i.e. create a duplicate copy of the Electronic Device's storage).

- 5.2 Often the data extracted will consist of messages sent to or from a relevant Participant, including information sent using SMS, WhatsApp and other instant messaging services, public or private posts and direct messages on social media, and emails. Relevant data may also include photos and videos, audio files including voice notes, call logs, contacts, documents, browser history, GPS location history, calendar entries and app-specific data, including metadata and other contextual information.
- 5.3 Once the data has been extracted, it will be provided to the Investigators on an Encrypted Device, such as a UFED, and the Investigators will then review the extracted data. The UFED is a leading digital intelligence platform used by law enforcement and forensic professionals to extract, unlock, and analyse data from Electronic Devices. In order to ensure security of the data, the extracted data can only be accessed on the Encrypted Device using an encryption key which is only made available to the relevant Investigators.
- 5.4 The Investigators will undertake targeted searches of the extracted data on the Encrypted Device using keywords, phrases, date ranges, or other targeted search techniques to identify material which is relevant to the investigation (and to remove or suppress irrelevant material). Once the relevant material has been identified, it will then be added to the investigation log and manually analysed by Investigators. The irrelevant material will remain on the Encrypted Device. If Investigators determine that further searches of the extracted data are required following an initial manual review of the relevant data, the Investigators will undertake further searches on the Encrypted Device.
- 5.5 The Investigators will not review all of the material extracted from Electronic Devices but rather, for reasons of efficiency and to respect your privacy, they will focus on that data and information which is relevant to their investigation. For example:
 - 5.5.1 for an investigation into an allegation of sexual misconduct or a serious safeguarding incident, the Investigators will search for information about an individual's sex life or sexual orientation, including unsolicited or non-consensual explicit images or messages;
 - 5.5.2 for an investigation into an allegation of corruption or serious financial misconduct (which is outside the scope of the Anti-Corruption Code), the Investigators may search for banking details and information about prohibited betting and gaming, and other financial transactions, including evidence of bribery or embezzlement of funds;
 - 5.5.3 for an investigation into an allegation of doping or the supply of prohibited substances, the Investigators may search for correspondence and information about prohibited performance enhancement, including the use or supply of drugs or attempts to evade testing protocols; and

- 5.5.4 for an investigation into an allegation of organised or systemic discrimination, the Investigators may search for information about an individual's racial or ethnic origin, religious or philosophical beliefs, or other personal characteristics, including evidence of the sharing of discriminatory or prejudiced messages, or communication of discriminatory views.
- 5.6 This process may involve the processing of special categories of personal data and/or personal data relating to criminal convictions or offences as defined by the UK GDPR. The Cricket Regulator relies on its legitimate interests (i.e. the interest inherent in its role overseeing and enforcing the Regulations) and, where necessary in respect of special category or criminal data, the Cricket Regulator will process that information for the establishment, exercise or defence of legal claims, or for reasons of substantial public interest (including for anti-doping purposes, to protect the integrity of sporting events, and to investigate or protect the public against unlawful acts, dishonesty, malpractice or other seriously improper conduct).
- 5.7 Any information extracted from the Electronic Devices will be used by the Cricket Regulator solely for the purposes of carrying out its investigations and, where relevant, the disciplinary process set out in the Regulations. All information will be kept strictly confidential, except where it becomes necessary to disclose the information to support a Charge, or where the information provides evidence of a breach of any applicable laws, regulations or rules, or where it is necessary to disclose the information to law enforcement bodies including the police, the courts or other competent authorities.
- 5.8 Participants (or their legal advisers) can request access to all data extracted from their Electronic Device as part of the disciplinary process outlined in the Regulation. Access to such data will be provided using an Encrypted Device.
- 5.9 Once the investigators are satisfied that the data extraction was successful, the Electronic Device will be returned to the Participant by hand delivery. If an "at venue" extraction was possible as outlined in paragraph 4.2, this will be on the same date that the Demand was issued. If an "at venue" extraction was not possible and the data from the Electronic Device were extracted by the third-party forensic partner as outlined in paragraph 4.3, the Electronic Device will be returned to the Participant after the extraction process has been completed, which could take a number of days. Please note that if the Cricket Regulator uncovers evidence of criminal activity as part of its investigation, the Cricket Regulator may provide the Electronic Device and the relevant data to law enforcement bodies including the police, the courts or other competent authorities.
- 5.10 All data that is extracted from the Electronic Device will be retained by the Cricket Regulator for no longer than is necessary for the purpose for which it was collected. In most cases, this will mean that the data is retained for the duration of the investigation, disciplinary process, and any subsequent appeal process. However, in certain circumstances, the Cricket Regulator may be required to retain the data for longer. This could happen, for example, where the extracted data contains or constitutes evidence of a breach of the Applicable Regulations by another Participant.