

INFORMATION SHARING PROTOCOL

between

THE LAWN TENNIS ASSOCIATION

and

Durham & Cleveland Lawn Tennis Association (D&CLTA)

THIS DOCUMENT (the **Protocol**) sets out the legal and practical basis on which the Lawn Tennis Association Limited (**LTA**) and Durham & Cleveland LTA (**the County**) agree to share, as a matter of policy, both routinely and incidentally, certain information that may be relevant to the safeguarding of children and vulnerable adults who participate in tennis nationwide.

The intention of this Protocol is to enable the LTA and the County (together the **Parties**) to share such information lawfully and securely, and with adequate safeguards for the privacy rights of individuals, but promptly and with confidence wherever appropriate. The Parties to this Protocol are mindful above all of the necessity of sharing appropriate information to create safer coaching and touring environments for children and adults at risk.

This Protocol is not a substitute for professional judgment and training, nor a practice-manual as to what information is to be shared. This Protocol is intended to provide a framework to establish the grounds for sharing lawfully. It is to be read alongside the LTA's Safeguarding Procedures (Appendix Two to the LTA Disciplinary Code) (the **Procedures**) and is drafted in compliance with the principles of the General Data Protection Regulation (**GDPR**) and the Data Protection Act 2018 (the **DPA 2018**): together (and alongside any supporting or implementing legislation) hereafter **Data Protection Law**.

The DPA 2018 requires data controllers to have in place appropriate policy documents to enable the proper handling of special category personal data for certain purposes, which is likely to include personal data processed for safeguarding purposes, and the Parties consider that this Protocol forms a part of the policy documentation achieving that aim.

1. The Parties

1.1 The Parties are:

Lawn Tennis Association Limited (company number 07459469) with its registered office at The National Tennis Centre, 100 Priory Lane, London, SW15 5JQ (the **LTA**); and

Durham & Cleveland LTA with its registered office at Durham & Cleveland LTA, Sunderland Tennis and Wellness Centre, Silksworth Lane, Sunderland, SR3 1PD

1.2 The Parties have each agreed to be bound by the terms of this Protocol (whether by direct acceptance of its terms or through adherence to the rules and policies of LTA governance). The Parties agree and acknowledge that by nature of their close relationship, shared goals and activities, they are ideally placed to contribute to this information sharing network and appropriate parties to it.

1.3 All Parties confirm that for the purposes of Data Protection Law they are data controllers in respect of certain personal information of individuals that may be of relevance to this Protocol (including of staff, coaches, players, parents and children), and have in place all appropriate policies and privacy notices reflecting their status as a data controller (including any notifications required to be made to the Information Commissioner).

1.4 The Parties likewise confirm they will adhere to Data Protection Law in relation to any personal data that may be subject to this Protocol, including without limitation: the use of appropriate technical and organisational measures to ensure the security of personal data; adequate, accurate and up-to-date record keeping; fairness and respect for individual's rights; and the requirement for a lawful purpose in any action in relation to that personal data, including information sharing. This Protocol sets out those legal purposes in section 3 below.

2. The Overriding Objective

2.1 The objective of this Protocol is to ensure that the Parties help create safer environments for children and adults at risk by sharing relevant information with relevant persons promptly and with confidence. By sharing in this way and in accordance with this Protocol, the Parties will be doing so in recognition of and compliance with the principles of data protection law.

2.2 Serious Case Reviews have highlighted that reluctance to share information because of legal concerns is a significant factor that contributes to avoidable outcomes.

2.3 In respect of any disclosures made by Parties to appropriate persons at the LTA, or by the LTA to any appropriate person at the other Party as may be appropriate, the Parties' overriding concern is to ensure that, while sharing is lawful and secure, the following applies:

- (i) if a disclosure is considered reasonably necessary by either Party for safeguarding purposes, then the disclosing Party **will** share that information; and
- (ii) no Party or individual using this Protocol should feel concerned or compromised by such sharing, provided the safeguards and rules in this Protocol are followed.

3. The legal basis for sharing

3.1 It is acknowledged by the Parties that:

- (i) the information relevant to this Protocol is likely to contain special category personal data within the meaning of GDPR (in particular, that relating to sexual life and physical or mental health records) and/or criminal records data as defined within the DPA 2018; and therefore
- (ii) while it is agreed that it is plainly in the legitimate interests of all Parties (and those they are bound to protect) to share safeguarding information for the purposes set out in this Protocol, in most cases an additional legal condition will also have to be satisfied under Article 9 GDPR (including the substantial public interest conditions set out in Schedule 1 Part 2 DPA 2018) and/or an additional condition relating to criminal convictions set out in Schedule 1 Part 3 DPA 2018.

3.2 It is also acknowledged that, while the explicit consent of the person whose information is to be shared would be sufficient, and seeking this should always be considered, obtaining it (or even seeking to do so) will in many cases be impossible, unreasonable (in the circumstances) or undesirable (in the sense of prejudicing the safeguarding aim or process).

3.3 Therefore, absent explicit consent of the individuals to whom any sensitive personal data relates, the following lawful grounds are agreed by the Parties for sharing of sensitive ('special category') personal information:

- (i) **Prevention of criminal activity.** Sharing of information may be necessary for the prevention or detection of crime (Schedule 2, Part 1 para. 2 of DPA 2018) – noting that whilst proper procedure will in many cases require that the police are fully involved at the right time, the Parties also have a role in prevention of crimes being committed against children and vulnerable adults under their duty of care;

- (ii) **Legal duties.** Sharing of information may be necessary because of duties imposed by law upon the Parties, including in connection with employment law (Article 9(2)(b) GDPR) – and for the purposes of this Protocol, the Parties agree that the law imposes duties on the LTA to protect those within its duty of care (noting Section B1 of its Procedures which states: "*The LTA has a duty to deal with all complaints and concerns about persons within its jurisdiction which raise protection issues about children or adults at risk*");
- (iii) **Legal rights and proceedings.** Sharing of information may be necessary in connection with actual or prospective legal proceedings, or to obtain legal advice, or by order of a court, or otherwise in connection with either party's or any person's legal rights or claims (Article 9(2)(f) GDPR / Schedule 2, Part 1 para. 5 of DPA 2018);
- (iv) **Protective functions and safeguarding.** Sharing of information may be necessary in circumstances where explicit consent is impossible, unreasonable or prejudicial to obtain, where either the LTA or another organisation requires the sharing for:
 - a. discharging a function in the public interest designed to protect the public (including children or vulnerable adults) from seriously improper conduct (Schedule 1, Part 2 paras. 11 and 12 DPA 2018); and/or
 - b. protecting children or vulnerable adults from physical, emotional or mental harm (including inappropriate sexual conduct), either as individuals or as a category of persons (Schedule 1, Part 2 para. 18 DPA 2018); or
 - c. Measures designed to protect the integrity of the sport, or any sporting event, from seriously improper conduct, including failure to comply with standards of behaviour set by a responsible Party (Schedule 1, Part 2 para. 28 DPA 2018).

Each of these purposes falls within a category of substantial public interest processing allowed for by Article 9(g) GDPR and subject to the safeguards herein. For these purposes, "children" are those under 18 and "vulnerable adults" are those at risk of harm owing to support or care needs, potentially including disabled players.

- (v) **Vital interests.** Urgent sharing of information may be necessary to protect the vital interests of a child or vulnerable adult (which may include sharing of the information of one person to protect a third party), where consent cannot reasonably be obtained in the circumstances (Article 9(2)(c)) – and HM Government guidance (referenced below) suggests that it may be sufficient that there are concerns that a child or vulnerable adult is suffering, or is likely to suffer significant harm.

3.4 Each of these grounds requires that sharing is "necessary" for the purpose. However, to be "necessary" it does not mean sharing this information is the only means to achieve the safeguarding aim, nor that sharing is at a particular time critical, urgent or unavoidable. The test is whether something is reasonably, rather than absolutely necessary: namely, is sharing the information a reasonable step to achieve the aim of protecting children or adults at risk (even if the risk is theoretical and the measure is preventative); and can the outcome be proportionately achieved without the personally identifiable data, or using less of it.

3.5 A safeguarding concern may in time prove to be groundless, but it does not render the act of sharing unnecessary or unlawful. In a safeguarding context, the sharing is only likely to be unnecessary if the information is irrelevant to the purpose, or too much information is provided carelessly or thoughtlessly (for example, identifying people without good cause), or it is carried out maliciously.

3.6 For the above reasons, the Parties consider that there will always be a lawful ground available for the sharing of even sensitive personal data between the Parties provided that a reasonable case can be made that the sharing was carried out in good faith for the purposes

of safeguarding children or adults at risk. As below, redactions and removals of names, including the attribution of pseudonymised or codified identifiers, should however always be considered, in particular to protect the identities of children – but is not required, and is to be avoided, if doing so is likely to materially decrease the efficacy of the safeguarding purpose.

4. When and what to share

4.1 The Procedures view safeguarding as a process of early intervention and prevention, to stop situations escalating. Part of this process is a question of relevant personnel being kept adequately informed to build a picture over time, especially when individuals (whether those who may be at risk, or those who may pose a risk) move to new homes or positions; it is also a question of relevant persons having access to appropriate historical files.

4.2 The Procedures also recognise that there are some situations that require swift intervention when a child, young person or adult at risk has been harmed or is likely to be harmed, and these situations call for rapid information sharing.

4.3 The Parties recognise that not every decision will be clear-cut, and it will not always be clear what information is relevant or even complete or accurate. However, the Overriding Objective of the Protocol is to ensure that Parties are not prevented from sharing potentially valuable information that may be critical to outcomes on the basis of uncertainty about the law. Provided that the sharing is with an appropriate person and for a good reason, this Protocol has set out that the law will support the sharing.

4.4 This Protocol is not intended to be a step guide or practice-manual as to when and what to share: these are decisions to be made in accordance with the Parties' existing rules, policies and procedures (including where applicable the Procedures) backed by professional experience and judgment. However, the framework this Protocol provides is intended to ensure that such professionals are taking that action promptly, securely and appropriately.

5. Who to share with

5.1 Both as part of fair and secure information sharing, but also to ensure the efficacy and speed of the process, it is vital that safeguarding information is only shared between the Parties via the appropriate person(s) who will:

- (a) be trained and qualified to exercise judgment about what to do with the information;
- (b) have access to relevant files and any other information that will inform that decision; and
- (c) understand how and where to keep the information securely and allow onwards sharing or access to others on a need-to-know basis only.

5.2 Each Party will have, within their organisational structure, a designated safeguarding lead role or officer.

5.3 In the case of all parties except the LTA, the name of the appropriate person should be notified to the LTA and kept up-to-date, including a deputy role or other senior decision-maker in the organisation with whom information may be shared safely in event of the lead's unavailability for any reason.

5.4 In the case of the LTA, the safeguarding team's details are as follows and in most circumstances it will be appropriate to share information with any if the same: T: 02084877000 / E: safeguarding@LTA.org.uk.

6. How to share personal data

6.1 Data Protection Law places great emphasis on the security of information in both how it is held and how it is shared: this includes who it is shared with, any by what means. Records should be kept of the sharing decision and process, as further set out at 7 below.

6.2 Determining what level of technical security is appropriate in sharing the data (by digital or physical means) is a factor of the risk of likely harm, both to individuals and to the safeguarding purpose, from the accidental loss of or unauthorised access, bearing in mind:

- (a) the volume, and nature (by its legal or personal sensitivity), of the information; and
- (b) the likely consequences of it being lost, or being accessed by the wrong person.

6.3 Whilst there is nothing inherently unlawful about, for example, the use of regular post or unencrypted email to share personal information, these methods of sharing information are plainly less secure than, say, contracted courier, personal service, or encrypted file transfer. Even special or recorded delivery may not be suitable, and the latter will require the intended recipient to be present (or the documents concerned may be retained in a depot).

6.4 Where digital files are sent by post (e.g. on a DVD or memory stick), email or FTP (file transfer Protocol), it is essential that consideration is given to whether the nature of the information requires that it should be password-protected. Given the likely sensitive nature of much of the information to be shared under this Protocol, this should be usual practice.

6.5 It is recommended that in most cases it will be useful, and more efficient, to have a telephone conversation first with the appropriate person to share any information or concern, then agree what if any additional material needs to be sent, and how best to send it (such that it will not be missed, delayed, left out, retained in a depot, or returned to sender).

6.6 Another principle of Data Protection Law is data minimisation. Because (absent consent) the lawful grounds to share personal data will depend on what is necessary to share, then it follows that the Parties should not share more than is necessary for that purpose.

6.7 Appropriate data minimisation may involve file review, redaction and, in some cases, de-identification of names: if it is clear that their identities are not necessary to include, or if the likely impact on their privacy is unwarranted by the likely benefit. However, that is provided that the overall value and purpose of the sharing is not compromised.

6.7 In event of any margin of doubt as to the necessity of sharing, the Parties should not risk prejudicing the value of the information or limiting its beneficial outcomes through excessive caution. Noting the Overriding Objective of this Protocol, and the Lawful Basis to Share established in section 3 above, lawful grounds are likely to exist to share data on a personal (full names) basis provided there is a safeguarding purpose to sharing the information.

6.8 Both physical couriers and digital or IT solution providers must be contracted under agreements that ensure integrity and security in compliance with Article 28 GDPR.

7. Record keeping around sharing

7.1 It is an important rule when sharing personal data (especially on an *ad hoc* basis) that the person sharing should establish certain conditions in writing with the recipient: namely the purpose of sharing, and the lawful grounds to share. This ought to be supported mutual promises of legal compliance with Data Protection Law, including secure retention or deletion, and any required limitations on onward use. This Protocol is intended to cover such issues when sharing as between the Parties, but the Parties must bear these principles in mind when sharing outside the Parties (for example, with police and local authorities).

7.2 Even when sharing between the Parties subject to this Protocol, there is great value both for future safeguarding purposes, and for legal risk mitigation, in keeping a dated record of:

- (i) what has been shared;
- (ii) with whom; and
- (iii) for what purpose.

7.3 This should include, where applicable, a record of any steps taken to secure, protect or minimise the personal data; any express limitations placed on the onward use of the information; and ideally a record of the legal basis for sharing. However, it is part of the intention of this Protocol that the Parties will not have to be specific on this last point provided that it is felt that the sharing falls within the intention and scope of the Protocol.

8. Respecting the rights of individuals

8.1 GDPR requires transparency (including the provision and availability of privacy notices: Articles 13 & 14 GDPR) and respect for the rights of data subjects (Articles 12-23 GDPR).

8.2 These rights include access to data and the right, in some cases, to rectify inaccurate data or object to or restrict processing. Safeguarding, GDPR and the DPA 2018 provide for particular exemptions to these rights – for example, concerning subject access:

- (i) because disclosure is not in the best interests of the data subject, in a context where the personal data consists of information about a child concerning whether he or she is or has been the subject of, or may be at risk of, child abuse (Schedule 3 Part 5 para.21 DPA 2018); or
- (ii) where there is a risk of serious harm in a medical or social care context (Schedule 3 Parts 2 & 3 DPA 2018), in which case the decision on disclosure should be referred to the opinion of the appropriate professional concerned; or
- (iii) in order to avoid prejudicing the basic protective function for which the data is being processed (Schedule 2 Part 2 para.7 DPA 2018), in this case safeguarding.

8.3 Where any of these may apply, the Parties must give due weight and consideration to applying them in favour of non-disclosure or redaction, with the overriding aim of protecting the integrity and efficacy of the relevant safeguarding process (and professional advice may need to be sought in a legal, social work, police or medical context). Where requests are received for erasure, the Parties should be aware of the available exceptions to this right and resist any request that would undermine the completeness, accuracy or efficacy of the file.

8.4 The sharing Party must also consider whether it is appropriate to notify affected individuals that their personal data is being shared, and with whom; and the receiving Party must similarly consider whether to so notify the individual(s) concerned that it is now data controller of their information.

8.5 There will of course be occasions where notifying affected individuals will be impossible, unreasonable for reasons of practicality, or inappropriate: for example if it would prejudice the safeguarding function. This is especially so if there is an ongoing police investigation, in which case the Parties must take great care not to “tip off” (inadvertently or otherwise) any person under suspicion, which may in itself be an offence.

9. Use and retention of personal data

9.1 All Parties agree that the sharing of personal information on the basis of this Protocol shall only be for the purposes intended by it, namely safeguarding children and adults at risk, and that no Party will use the personal information for any incompatible purpose nor keep it for any longer than is necessary for the intended purpose or purposes it was shared.

9.2 The purposes for which it is agreed the information shared under this Protocol may be used and retained will include: preventative or reactive steps to safeguard individual children or adults at risk, or groups or categories of the same; creating safer environments and improving safeguarding practices; historic case files for the purposes of future claims, case reviews, legal advice and insurance purposes, or official and internal inquiries; regulatory reasons; upholding or enforcing legal rights of individuals; and cooperation with authorities. The Parties agree that such purposes may require long retention periods, during which the information will continue to be kept securely and accessed on a need-to-know basis only.

9.3 The Parties agree that, provided that any information shared is only used for purposes compatible with the overriding safeguarding purpose of sharing. Onward uses may include sharing with police or local authorities, or other Parties, or future employers or other organisations, if the safeguarding circumstances require it. Any onward uses of the personal data by appropriate persons shall be a matter for the receiving Party to determine as data controller, but each Party strictly agrees to do so only as necessary for a lawful purpose, subject to Data Protection Law, and by reference to the principles set out in this Protocol.

9.4 The legal rights of individuals under Data Protection Law, including the right to access personal data, will similarly bind on the receiving party (whether or not a Party to this Protocol) and may involve the receiving party revealing the source of the information.

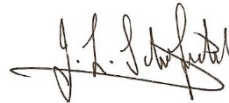
10. Enquiries

10.2 In case of any doubt as to the application of this Protocol, or if any queries arise from it, please contact the Safeguarding Team on 02084877000 or safeguarding@lta.org.uk.

Signed for and on behalf of the LTA: *Mathew Lea*

Date: 14/12/2020

Signed for and on behalf of the County:



(President)

Date: 23rd November 2020