VIBRANT NATION

Managing and Sharing Safeguarding Data in Sport

VIBRANT NATION

Contents

A quick comment about SARs

We are going to re-iterate something that we say a lot when discussing safeguarding. Data protection law is top of the list when it comes to confusion and uncertainty when dealing with a request for safeguarding information.

Don't get a request for safeguarding information from another authority or organisation mixed up with a SAR. The provision of safeguarding information to the police or social services for example, is not to do with a SAR and is permitted. Always seek advice if you are not sure.

It cannot be stressed enough that a request for safeguarding information from another organisation or other authority such as the police or social services is not a subject access request.

Data protection law

There are several areas of law that need navigating when dealing with safeguarding information about children or adults at risk. The most commonly quoted legislation is the General Data Protection Regulation (GDPR) along with the Data Protection Act 2018 (DPA2018). We must treat any information that we hear regarding the GDPR and the DPA2018 with extreme caution when we are dealing with safeguarding data. Many people will outline the restrictions of these two laws and explain why you cannot share your information about a concern. This type of advice is invariably wrong.

A detailed reading of the GDPR and the DPA2018, which should always be considered together, will disclose key provisions for the reporting of safeguarding concerns and the sharing of information. If there is a need to act to protect the welfare of a child or adult at risk, **you do not need consent** from anyone involved. A key theme that underpins much of what we do in safeguarding is:

The safety and wellbeing of the child or adult at risk is paramount

This must always be remembered when we make decisions about safeguarding data and sharing.

Making a decision

It is better to have a process to guide the decision making. This will allow a more consistent approach and will help staff to divorce themselves from the emotional and personal aspects of a situation and to focus on objectivity. Each case that is dealt with will vary in the degree of impact on the young person, the urgency of the situation, the circumstances and source of the harm, and the other agencies that are or may need to get involved. It can be easy to make a judgement outside of a methodical approach and get it badly wrong.

Having a process will also ensure that you have all the information that you need and that you have also controlled this information correctly. Controlling the information is vital to protect people's privacy and not cause distress or further harm to anyone involved.

When designing or implementing a process to help guide decision makers, you must ensure that it is not overly prescriptive. Always remember that each safeguarding issue will have unique attributes and your process needs to allow for this.

Guiding considerations

Professor Eileen Munroe produced a report after her review into child protection in 2011. She points out there is a strong case for measures that can prevent child abuse rather than only considering reactionary measures once abuse occurs. It is clear then that preventative services do far more to reduce abuse than reactionary services do. The report stresses the importance of early help and intervention. Early help can only be achieved by the sharing of early concerns with other agencies. The United Nations Convention on the Rights of the Child (CRC) and the Children Act 1989 both support the moral argument that adverse experiences in childhood should be minimised. It is also widely accepted that an adverse experience in childhood causes long term effects and this damage is very difficult to reverse.

It is a sad fact that when serious cases that have resulted in death or serious injury of a child, the lack of, or poor information sharing is a repeated factor.

We must not allow fear of sharing information stand in the way of safeguarding and protecting the welfare of children at risk of neglect or abuse. We must all take responsibility and never assume that someone else has passed on information which might be essential to keep a child safe from harm.

Pointers

Here are seven things to bear in mind when making a sharing or disclosure decision. These points are derived from government issued guidance documents on the sharing of safeguarding information.

1	Remember that the General Data Protection Regulation, Data Protection Act 2018 and human rights law are not barriers to information sharing where it is justified and appropriate. They provide a framework to ensure that personal information about living individuals is shared correctly and lawfully.
2	Be open and honest with the individuals and/or their families where appropriate from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement*, unless it is unsafe or inappropriate to do so.
3	Seek advice from other safeguarding leads, or your information governance lead, if you are in any doubt about sharing the information concerned. Avoid disclosing the identity of the individuals concerned where possible.
4	Gain consent* from individuals where it is appropriate to do so. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. Where you do not have consent, be mindful that an individual might not expect information to be shared.
5	Consider safety and well-being. Base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions. Will your sharing of the information cause harm to a child or adult at risk?
6	Necessary, proportionate, relevant, adequate, accurate, timely and secure are key elements of sharing. ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up to date, is shared in a timely fashion, and is shared securely.
7	Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

* We will look at the issue of consent next. Don't place any particular emphasis on consent in a safeguarding context.

The issue of using consent

We see a lot of use of the word 'consent' in guidance produced by both National and Welsh government regarding the sharing of safeguarding data. Much of the advice will suggest seeking consent as a primary measure to authorise the sharing of safeguarding data when you are able to do this. Consent, though, is a tricky issue especially if it is the consent of someone under the age of 18. Consent in data protection law is also frequently unclear to the untrained reader and can be confusing with an array of ages and circumstances that constitute whether someone is a child or not.

Although generally anyone under the age of 18 is classed as a child, UK data protection law has reduced this age to anyone under 13 years of age with regards to the *giving of consent* to *data processing for information society services*. In essence, this really means that someone who is 13 years or older can sign up to an online service such as Instagram, Twitter, WhatsApp etc. and legally give consent for their personal information to be collected and processed. This can lead to a lot of confusion over the status of a child and it is very important to treat data protection issues separately from other issues when judging if someone is a child or not. Safeguarding clearly does not fall under the definitions of a child in the GDPR or DPA2018 and so a child in the current context is anyone under the age of 18.

Another important aspect of consent under the GDPR is that consent must be *freely given*. We must always look at the relationship between the person requesting the consent and the person giving it. If it were an employer asking an employee for consent for something work related, then it would be considered that this consent would **not** be freely given due to the inequitable power balance of the relationship. Generally, in data protection matters, we only use consent if there are no other legal bases for processing.

Finally, where consent is used to process or share data, this consent can be withdrawn. This is likely to be very problematic if it happens after safeguarding information sharing has occurred.

In summary then, the use of consent to share safeguarding information should be **avoided** where it is lawful to do so.

Never tell a child you will keep a disclosure they have made a secret. Always be honest that you will need to tell someone to get them the help they need and deserve.

We will look at how and when safeguarding data can be lawfully shared without consent and even without the knowledge of those involved.

Safeguarding without consent

When we consider the processing of personal information in a safeguarding context, we can be talking about three different classes of data subject: The child or adult of concern, the potential or alleged abuser and the reporter(s) of a concern. We need to treat each of these classes of person in a slightly different way when considering the sharing of a concern with another agency.

The reporter

A person who reports a concern may report about a child they consider might be at risk, or they may report the behaviour of staff or volunteers, or possibly another third-party that may give rise to a case of abuse or neglect. It is important that the rights of the reporter are respected under data protection law. If the concern has been reported anonymously, it is often a simple task to identify who the reporter might be. This should not be undertaken under any circumstances. By making an anonymous report, the reporter has demonstrated that they do not wish to be identified. If identification is subsequently made, this will have a catastrophic effect on reporting of concerns within your organisation as well as giving rise to complaints in law.

If the report is not anonymous, the confidentiality of the report must be maintained and kept secure. If a decision is made to share a concern with another agency, the consent of the reporter for their name to go forward should be sought and their wish should be respected unless it would cause a detriment to the welfare of the child concerned.

Whistleblowers

It is possible that a report of concern that you receive may be about the behaviour of one of the staff or volunteers. This report may be from another member of staff. This is, in effect, whistleblowing. This type of situation needs to be handled carefully. Whistleblowers are afforded protection under the Pubic Interest Disclosure Act which alters employment laws concerning any reprisals or other detriments in the workplace as a consequence of reporting concerns. Organisations have a duty to protect those that blow the whistle on bad practices. Again, any failure to protect the interests of a whistleblower may well discourage the reporting of genuine concerns and this may be detrimental to children and adults at risk.

The potential or alleged perpetrator

We are not going to cover any part of the process for investigating someone who has been reported for their behaviour in a safeguarding context. We will consider how their information is handled though.

The considerations will need to be whether they are informed or not and the amount of detail they are given about any allegation. Always remember **the welfare of the child is paramount**. You may choose to not disclose anything to the alleged perpetrator at all.

You are legally able to process this kind of information in compliance with data protection law if disclosing this to a person or persons concerned would likely prejudice your aim of safeguarding the child or adult at risk. You are permitted under the DPA2018 Schedule 1 paragraph 18 (See appendix) to process this information without consent.

The child potentially at risk

If the child or adult at risk has not personally disclosed the abuse or neglect, you must be cautious of informing them that a concern has been raised about them as this may cause them incalculable emotional harm or distress. This is a judgement best left to safeguarding leads or local agencies. The information that is recorded should be guarded very carefully. Security of the information is vital to protect the welfare of the child and to respect the welfare of those who may be accused of neglect or abuse – there is a due process and culpability must never be assumed or proscribed outside of the process.

If a child or adult at risk discloses information to you, be very clear about what will happen next. Do not ask for their permission to report the concern, if they specifically ask you to keep it a secret do NOT agree to.

Under data protection law, this type of information can be processed without the consent of the child or adult at risk where there is a reasonable concern for their welfare. This is permitted under the DPA2018 Schedule 1 paragraph 18 (See appendix).

Principles for sharing

Requests for information

It may be the case that you are approached by another agency, maybe social services or a school, and asked to provide information about on ongoing concern they may be working on. It is important that this request is handled by the safeguarding lead. **It is very important that the requestor is verified and checked to ensure they are legitimate.** It is very possible the request may be someone posing as an official to gain information about a child. If a child is in care or under a court order, failure to vet the requestor may result in harm coming to the child or another person.

Do not be persuaded that you must or must not share information 'because of GDPR' or 'data protection'. The law provides for reasonable decisions to be made to either share information or in some case to withhold information as we have already examined. **There is no barrier in law to sharing information with the police or social services.**

Always remember our key consideration: **The safety and wellbeing of the child or adult at risk is paramount**

Deciding to share

There are many guides issued by the Welsh government and the NSPCC Child Protection in Sport Unit that cover the topic of when to share information and who to share it with. Structures are usually in place locally and your safeguarding lead will know how to report a concern to the wider agencies. We will only advise to consult the latest information available and follow guidance provided.

Having made a decision to share information regarding a safeguarding issue, we now turn our attention to consider what information, the amount of information, and how it should be shared.

Necessity and proportionality

Consideration should be given to the amount of information that should be shared to achieve the desired outcome in a safeguarding situation. The amount of information disclosed should be kept to the minimum required and consideration must also be given to any third parties and the impact upon them. The level of risk to the individual needs to be assessed and the response and sharing should be proportionate to the risk of the situation.

Adequacy and accuracy

The information that is shared must be checked for accuracy. It must also be adequate in its quality as well as the quantity so that it can be relied upon. Make sure that the information is about the FACTS rather than an opinion of someone. Also ensure that the chronology of information is included so that current and historical facts are clearly identified.

Relevancy

Restrict the shared information to only what is relevant for the recipient. This will assist in both clarity and the making of correctly informed decisions.

Promptness

Avoid any delays in sharing information. If the matter is urgent, and the situation serious share the information quickly. ideally concerns should be reported **within 24 hours**. Be certain to make use of every opportunity to offer support and protection to a child that needs it.

Accountability

Always record what information has been shared and with whom. Also record the rationale for the sharing and the process and thinking behind any decision. Keep this record secure. If a decision is made to not share information, again record this in a similar manner. These records should be retained for as long as they are required, this may well be indefinitely and will depend on the circumstances of the situation.

Securely sharing information

It is preferable for organisations to consider the method of sharing safeguarding data and write preferred methods into the safeguarding policy. When information is being transferred from one organisation to another, it is at its most likely point of being lost or stolen in some way.

Paper files left in a car, even for a brief period, may be stolen. We have seen recent reports of disks containing thousands of staff payroll records being stolen from a car – it does happen.

Emails are prone to being intercepted or accidently sent to the wrong person. If the sensitive content is not encrypted, it is not secure and may be accessed by someone without authority.

Here are some ways of sharing data securely:

Encrypted email attachment

Place the material into a folder on your computer and compress or 'zip' the folder with a password. Give the file an innocuous name and email it to the recipient. Do NOT include the password on ANY email to them, they mail have had their email compromised and a hacker may see a copy of all their emails. Give them the password over the phone or via the regular post. Never discuss safeguarding specifics over unencrypted or insecure emails.

By post or in person on a USB drive

Place the information into a zip file as above and password protect it when it is being compressed. Then place the file on a USB flash drive and post it or take it to the recipient. Once they have received the drive, give them the password verbally.

On paper in person

Print the required information and insert it into a strong envelope. Seal the envelope with a tamper proof security seal and hand deliver the papers to the correct recipient in person. If travelling by car, put the papers in the boot of the car (never on the seats) and go directly to meet them. If you travel via public transport, place the envelope into a closed bag and keep a hand on the bag at all times until you have handed over the contents to the recipient in person.

Secure transfer service

There are several secure transfer services on the internet. Use an encrypted file as before and use the transfer service to deliver it. Once delivered, delete the file from the service. Give the password verbally once the file has been received safely.

Securely storing safeguarding information

Consider the digital or physical security of safeguarding information. Keep papers locked away and control access to them. If information is stored on a computer, consider encrypting this information with a strong password and make sure access to the computer is password protected. Ensure that backups of the information are made and that these backups are also encrypted with password protection.

If you are in any doubt about how secure you need to keep information that concerns safeguarding issues, imagine the damage that would be caused if the information were to be stolen and placed all over the internet. Imagine the damage to your organisation, personal reputations and above all else the catastrophic harm it may cause to a child or adult at risk. You need to be able to ensure as far as possible that this cannot happen.

Dealing with a SAR and safeguarding information

There are three basic areas that a person (a data subject) may be involved in a safeguarding issue and be a subject in any information about the issue: The reporter of a concern; the alleged perpetrator of a concern; or a child or adult at risk who is the subject of a concern. When responding to a SAR, it must be remembered that priority should be given to the welfare of the child or adult at risk concerned. It may not be in their best interests to release information about an issue. You need to be cautious about any attempt to 'anonymise' any information as this is not always possible. Often the circumstances of a case are sufficient to identify the persons involved.

An allegation about a potential perpetrator of safeguarding issues may also quickly lead to the identity of the child or adult at risk concerned. Even if the person making a SAR knows there is an allegation involving them, remember this may well be the reason for the SAR, giving any detail about the allegation could lead to the identification of either the child at risk or the informant. For example, even a simple date when an incident is supposed to have occurred could lead indirectly to the identification of other persons that are involved.

There is an equal consideration to be made if the SAR comes from the child or adult at risk. If it is not in their best interests, then information should be withheld.

There is an exemption in the Data Protection Act 2018 from disclosing safeguarding data about a child under the age of 18 or an older person that does not have capacity to manage

their own affairs. It is outlined in Schedule 3 paragraph 21 (see appendix). You are not obliged to confirm the fact that you are processing safeguarding information nor are you obliged to provide the data subject or their representative any access to such data. Additionally, you are not required to notify the data subject if safeguarding data concerning them is transferred internationally. This is regardless of their involvement in a concern.

Withholding under this exemption is permitted if releasing the information would not be in the best interests of the data subject or the person who is deemed to be at risk. This exemption also applies to the legal guardian of the data subject as well.

Summary

We must always remember our key consideration: **The safety and wellbeing of the child or adult at risk is paramount.**

Ensure that your safeguarding processes include dealing with requests for information from other agencies. Ensure that the relevant staff understand that these requests are not subject access requests and the data protection law allows the information to be given.

Be clear about processing safeguarding information and how the law allows this without the consent of individuals involved where this is appropriate. Never refrain from recording or reporting a concern due to fear over data protection law, it is never a barrier to the welfare of a child. **Timely reports result in better outcomes.**

Never agree to keep a disclosure by a child or adult at risk a secret. Always be honest about the next steps and the need to report the concern to enable the individual to get the help they need and deserve.

Respect the anonymity of reporters and whistleblowers. Ensure that your staff and volunteers can raise concerns confidently and confidentially.

When you share a concern make sure you share good information that is about facts and this is done securely. Store your safeguarding information securely and control access to it carefully.

If you receive a subject access request, always remember that you do not have to mention anything about safeguarding information if this would jeopardise the welfare of a child or other individual concerned (including people who have reported concerns).

If you are ever in any doubt, GET ADVICE.

Useful information

Welsh Assembly Government: Information sharing guidance
https://gov.wales/sites/default/files/publications/2019-07/working-together-to-safeguard-people-information-sharing-to-safeguard-children.pdf

Welsh Assembly Government: Safeguarding children.
https://gov.wales/safeguarding-children

Social Care and Wellbeing (Wales) Act 2014
http://www.legislation.gov.uk/anaw/2014/4/contents

NSPCC Learning: Child protection system in the UK.
https://learning.nspcc.org.uk/child-protection-system/

NSPCC Child Protection in Sport Unit Resource Library.
https://thecpsu.org.uk/resource-library/

Appendix

DPA2018 Schedule 1 paragraph 18

Safeguarding of children and of individuals at risk

(1) This condition is met if

(a) the processing is necessary for the purposes of

(i) protecting an individual from neglect or physical, mental or emotional harm, or

(ii) protecting the physical, mental or emotional well-being of an individual,

(b) the individual is

(i) aged under 18, or

(ii) aged 18 or over and at risk,

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(d) the processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(c) are

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in subparagraph (1)(a).

(3) For the purposes of this paragraph, an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual

(a) has needs for care and support,

(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and

(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.

DPA2018 Schedule 3 paragraph 21

Exemption from Article 15 of the GDPR: child abuse data

(1) This paragraph applies where a request for child abuse data is made in exercise of a power conferred by an enactment or rule of law and

(a) the data subject is an individual aged under 18 and the person making the request has parental responsibility for the data subject, or

(b) the data subject is incapable of managing his or her own affairs and the person making the request has been appointed by a court to manage those affairs.

(2) Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) do not apply to child abuse data to the extent that the application of that provision would not be in the best interests of the data subject.

(3) "Child abuse data" is personal data consisting of information as to whether the data subject is or has been the subject of, or may be at risk of, child abuse.

(4) For this purpose, "child abuse" includes physical injury (other than accidental injury) to, and physical and emotional neglect, ill-treatment and sexual abuse of, an individual aged under 18.

(5) This paragraph does not apply in relation to Scotland.