CCTV AND ACCESS CONTROL PRIVACY NOTICE

WHY DO WE HAVE THIS PRIVACY NOTICE?

We are Gymshark and treating individuals and their personal information with respect reflects our core values and the values of our brand(s). So we want you to know as much as possible about what we do with your personal information. Also you and your personal information are protected by various laws and guidance and Gymshark is committed to upholding these and respecting your privacy and keeping your information safe. So whilst this privacy notice is quite long, we want you to be fully informed. Please note while you read it, that not all parts of this privacy notice may apply to you depending upon whether you are a member of our staff, you do not use our Access Control systems or you manage to visit our premises without being recorded on our CCTV system.

In this privacy notice any reference to "us", "we", "our" or "ourselves" is a reference to Gymshark, and the particular part of the Gymshark group whose premises you visit and any reference to "you", "your" and "yourself" is a reference to you as a visitor to our premises.

This privacy notice applies to any visitors to or a member of our staff using Gymshark's premises whose images are captured on our CCTV systems and/or who use our Access Control systems at our premises usually a key card, fob or code entry system. You may be applying to work for us, or already work for us as one of our staff as an employee, director, temporary worker or consultant. You may also be a representative of a supplier to us, a customer of ours or on our premises for any other reason. This privacy notice provides details, in accordance with data protection laws, about how we collect and use personal information about you on our CCTV and Access Control systems during and after your visit to or use of our premises. Depending on the reasons for your visit to or use of our premises, you may also be covered by another privacy notice as well as this one.

Please note we have a separate Rest of the World privacy notice that applies generally to individuals when they are external to our business, including users of our website, a copy of which can be found at https://www.gymshark.com/pages/gymshark-privacy-notice . We also have a separate privacy notice that applies to our customers and potential customers, a copy of which can be found at https://www.gymshark.com/pages/gymshark-privacy-notice , so this will apply if you purchase products from us, use our Gymshark app(s), add yourself to our marketing database, enter any of our promotions/competitions, apply to attend any of our events or you have an unpaid active social media relationship with us. We also have a separate privacy notice that will apply to you if you apply to work for us, which will be provided to you during the recruitment process. You should also read these privacy notices to the extent that they will apply to your activities as they may apply to you in addition to this privacy notice.

THE CONTROLLER OF YOUR PERSONAL INFORMATION

For the purposes of data protection laws and this privacy notice, whichever part of the Gymshark group is processing your personal information is the controller of your personal information for that processing of your personal information. This will usually be the part of the Gymshark group that controls the premises that you are visiting. Being a controller of your personal information means that we are responsible for deciding how we hold and use your personal information. Our main trading entity is Gymshark Limited (Reg No. 08130873) which is incorporated in England and Wales. If you are visiting our premises in the UK then this company will be the controller of your personal information. If you are visiting premises outside of the UK then the controller of your personal information will be the part of our group that controls those premises. Details of its identity will also be contained on CCTV warning signs at and around the premises. Sometimes we may pass personal information to different parts of our group, so this privacy notice covers our whole group and more than one part of our group may be a controller of your personal information. Regardless of which premises you visit and regardless of which part of our group may be a controller of your personal information, any queries you have regarding your personal information will be dealt with by Gymshark Limited, which can be contacted at dpo@gymshark.com.

WHAT IF YOU DO NOT PROVIDE PERSONAL INFORMATION?

Failing to provide some of the personal information we require may mean that you are not allowed to access our premises using our Access Control systems. The only way not to have personal information captured by our CCTV systems is to stay out of the line of vision and range of our CCTV cameras.

IF YOU HAVE QUERIES OR CONCERNS JUST ASK!

We have appointed a data protection officer (DPO) to oversee our compliance with data protection laws. If you have any questions about this privacy notice or how we handle your personal information, please contact our DPO on dpo@gymshark.com.

CHANGES TO THIS NOTICE

We keep our privacy notice under regular review and we may update this privacy notice at any time. The current version of this notice is available on our website at https://www.gymshark.com/pages/gymshark-privacy-notice or by requesting a copy from dpo@gymshark.com. If there are any material changes to this privacy notice in the future we will let you know, usually by updating the version on our website.

DATA PROTECTION PRINCIPLES

We are committed to being transparent about how we collect and use your personal information and in meeting our data protection obligations. Data protection laws say that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

To make sure this happens we are required under data protection laws to notify you of the information contained in this privacy notice. It is important that you read this document before you visit our premises so that you understand how and why we will process your personal information.

WHAT PERSONAL INFORMATION DO WE COLLECT?

As a visitor to or a member of our staff using our premises we may collect and process certain personal information about you in our CCTV system and our Access Control systems. As a visitor you may not always make use of our Access Control systems, but it will be difficult for you to avoid personal data being captured by our CCTV system. The types of personal information we may collect are:

- CCTV - we may collect from you video recordings and still pictures which feature you if you are in the field of vision of any of our CCTV system. This personal information may include your activities, your face, clothing, possessions, car registration, colour, make and model details and other visual information about you which is recorded on our CCTV system.
- Access Control system - Personal contact details such as name, title, address, email address and telephone number(s) when we issue you with a fob, key card, code or other similar means to use our Access Control system, and then when it is being used it may record times, dates, location and link these to your identity each time the Access Control system is used by you.
- Any communications between ourselves and you relating to our CCTV and Access Control systems.
- Details of any claims or disputes relating to you and our CCTV and Access Control systems.
- Any other personal information provided by you.

WHERE DO WE COLLECT YOUR PERSONAL INFORMATION FROM?

We collect your personal information in our CCTV systems and Access Control systems directly from you as you are on and move around our premises. We do not generally use these systems to collect your personal information from third parties, though in some cases we may collect the personal information from a third -party provider of CCTV and/or Access Control systems to us.

WHAT ARE OUR BASES FOR PROCESSING YOUR PERSONAL INFORMATION?

We will only use your personal information when the law allows us to. This means we must have one or more legal bases to use your personal information. Most of these will be self-explanatory. The most common legal bases which will apply to our use of your personal information are set out below:

- Where we need to perform the contract, we have entered into with you which covers your working relationship with us or to take steps to enter into that contract.
- Where we need to comply with a legal obligation which applies to us, for example complying with health and safety laws.
- Where it is necessary for legitimate interests pursued by us or a third party and your interests and fundamental rights do not override those interests. We have set out in the section below how we use your personal information together with more details on our legitimate interests.

Whilst this is almost always not the case with our CCTV systems and Access Control systems, if we are processing any sensitive special category personal information about you (which covers personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation) then we also need to have one or more of the following bases for using your personal information.

- Where it is necessary for us to comply with our obligations and exercising our rights in the field of employment law, social security law and social protection law.
- Where we need to protect your vital interests (or someone else's vital interests).
- Where you have already made public the personal information.
- In establishing, exercising or defending legal claims, whether those claims are against us or by us.
- Where it is necessary in the public interest.

We will not usually process any of these types of special category personal information about you, and in cases where we do process special category personal information about you it will generally be to comply with legal obligations, where you have given your consent or to establish, exercising or defending legal claims. In some cases more than one legal basis may apply to our use of your personal information, so for example it may be in our legitimate interests to use an Access Control system and it may also be to comply with legal obligations, for example health and safety obligations to keep our premises and staff safe.

HOW WILL WE USE YOUR PERSONAL INFORMATION?

There are many ways we will need to use your personal information and we have set out the main uses below and indicated the main applicable legal bases of processing, but there may be other specific uses which are linked to or covered by the uses below.

- For the prevention, detection and prosecution of crime, which is in our legitimate interests, in the public interest, and in some cases may also be a legal obligation.
- For evidence in any civil or criminal legal proceedings, and if you work for us, in any disciplinary or grievance proceedings and taking decisions in relation to any such proceedings. As well as relating to the entry into or performance of an existing contract with you either directly or indirectly, this will also be in our legitimate interests. We may also have a legal obligation to do so, be exercising a legal right to do this and it may also be needed to establish, bring or defend legal claims.

- To assist in investigations, which is in our legitimate interests, in the public interest, and also in some cases may be a legal obligation.

- For safety and security, for example to comply with health and safety laws and this is also in our legitimate interests.

- Dealing with any claims, queries, complaints or enquiries and to manage our relationship with you, which may relate to the entry into or performance of an existing contract with you either directly or indirectly, or be in our legitimate interests. We may also have a legal obligation to do so or be exercising a legal right to do this and it may also be needed to establish, bring or defend legal claims.

- We may need to process your personal information to help train our staff, and make sure they deliver the high standards expected in relation to our brand. This will be in our legitimate interests.

- Retaining records, which will be in our legitimate interests, may be in the public interest and in some cases we may have a legal obligation to do so.

- To manage our CCTV and Access Control systems to ensure compliance with our information technology policies, ensure network and information security, including preventing unauthorised access. This will also be in our legitimate interests and we may also have legal obligations or be exercising a legal right to do this.

We may anonymise any of the personal information we hold on our CCTV system or Access Control system (so that it does not directly identify you, for example by obscuring your face) and it therefore ceases to be your personal information. We may use this anonymised information for any other purposes.

CHANGE OF PURPOSE

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law. We will rarely need to rely on your consent to process any of your personal information in our CCTV and Access Control systems.

AUTOMATED DECISION-MAKING

Automated decision making takes place when an electronic system uses personal information to make a decision about that person without any human intervention which produces legal effects concerning them or similarly significantly affects them. We do not currently use this type of automated decision making in our business in relation to our CCTV and Access Control systems.

WHO HAS INTERNAL ACCESS TO YOUR PERSONAL INFORMATION?

Your personal information may be shared internally with our staff, including with members of our facilities team, the People and Talent team, managers and senior staff, the tech and legal teams where access to your personal information is necessary for the performance of their roles. We only provide access to your personal information to those of our staff who need to have access to your personal information.

WHO DO WE SHARE YOUR PERSONAL INFORMATION WITH EXTERNALLY?

When using your personal information we may share it with third parties, but we will only do so when it is appropriate and we have a legal basis for doing so. Third parties that we may share your personal information with include:

- Any third party approved by you.

- An organisation you work for or that represents you if that organisation has a relationship with us.

- Service or product providers to our business, for example information technology services suppliers, CCTV or Access Control suppliers and third parties that process personal information on our behalf and in accordance with our instructions.
- People who have been injured, attacked or had property damaged or stolen and their insurance providers to assist them with any criminal or civil investigations or legal proceedings.
- People who have been involved in road traffic accidents and their insurance providers: to assist with insurance claims, legal claims and investigations.
- Private and other investigators to aid their investigations.
- Another company within our group of companies, especially if we are dealing with any enquiry, claim, complaint, disciplinary or grievance proceedings and it is relevant to do so.
- Purchasers, investors, funders and their advisers if we sell all or part of our business, assets or shares or restructure whether by merger, re-organisation or in another way.
- Our legal and other professional advisers, or any professional advisors appointed by you, for example a legal advisor.
- Governmental bodies, regulators, police, law enforcement agencies, security services, courts/tribunals.

INTERNATIONAL TRANSFERS

It is sometimes necessary to share your personal information outside of the UK and the European Economic Area (the EEA) or it will be collected outside of the UK and the EEA. This will typically occur when service providers to our business are located outside the EEA or if you are based outside the EEA. These transfers are subject to special rules under data protection laws.

The same applies to any transfer of personal information to another part of our group of companies based outside of the UK and the EEA. We also apply the same standards to any transfer of personal information between members of our group, regardless of where the group company is based.

If we transfer your personal information outside of the UK and the EEA, we will ensure that the transfer will be compliant with data protection laws and all personal information will be secure. Our standard practice is to assess the laws and practices of the destination country and relevant service provider and the security measures that are to be taken as regards the personal information in the overseas location; alternatively, we use standard data protection clauses. This means that when a transfer such as this takes place you can expect a similar degree of protection in respect of your personal information.

Our directors and other key staff working for us may in limited circumstances access personal information from outside of the UK and EEA if they are on holiday abroad outside of the UK or EEA. If they do so they will be using our security measures and the same legal protections will apply that would apply to accessing personal information from our premises.

Depending on the circumstances the people to whom we may disclose your personal information may be located outside of the UK and EEA and we will not have an existing relationship with them, for example a police force in a country where we have premises outside of the UK and EEA. In these cases, we will impose any legally required protections to the personal information as required by law before it is disclosed.

If you would like any more details about how we protect your personal information in relation to international transfers then please contact our DPO at dpo@gymshark.com.

HOW DO WE PROTECT YOUR PERSONAL INFORMATION?

We are committed to keeping your personal information safe and secure and so we have numerous security measures in place to protect against the loss, misuse, and alteration of information under our

control. We will always aim to use best in class security systems implemented across our networks and hardware to ensure access and information are protected. Our security measures include:

- Encryption of personal information where appropriate.
- Regular cyber security assessments of all service providers who may handle your personal information.
- Regular planning and assessments to ensure we are ready to respond to cyber security attacks and data security incidents.
- Regular penetration testing of systems.
- Security controls which protect our information technology systems infrastructure and our premises from external attack and unauthorised access.
- Regular backups of information technology systems data with functionality to correct errors or accidental deletion/modification to data.
- Internal policies setting out our information security rules for our staff.
- Regular training for our staff to ensure staff understand the appropriate use and processing of personal information.
- Where we engage third parties to process personal information on our behalf, they do so on the basis of our written instructions, they are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of personal information.

We take information security very seriously and will use all reasonable endeavours to protect the integrity and security of the personal information we collect about you.

FOR HOW LONG DO WE KEEP YOUR PERSONAL INFORMATION?

We will hold your personal information on our CCTV system until it is overwritten on the storage media we use, which is generally between 14 - 30 days depending on the CCTV system.

We will hold your personal information on our Access Control system until it is no longer required for the purpose(s) for which it was collected at which point it will be anonymised and/or deleted where required.

In either case if your personal information becomes or is thought to be relevant to any matters we may extract or copy it from our CCTV or Access Control system and retain it separately. In this case it will be retained for as long as it remains relevant to that matter. For example, if the personal information is relevant for a dispute or legal claim, it may be retained for the duration of that process, which might take a number of years.

We will not retain your personal information for longer than necessary for the purposes for which it was collected and for which it is being used. We do not guarantee to retain your personal information for the whole of the periods set out above, they are usually the maximum period.

YOUR RIGHTS

As an individual whose personal information we collect and process, you have a number of rights. You may:

- Withdraw any consent you have given to us, although this will only be relevant where we are relying on your consent as a basis to use your personal information, but it is an absolute right. This is not usually relevant to personal information in our CCTV and Access Control systems.
- Request details about how your personal information is being used. This right is linked with the right of access mentioned below.

- Request access and obtain details of your personal information that we hold (this is commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- Request erasure of your personal information. This means that you can ask us to delete or stop processing your personal information, for example where we no longer have a reason to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (set out below). The right to have data erased does not apply in all circumstances.

- Object to the processing of your personal information where we are relying on a legitimate interest (ours or that of a third party) and there is something about your particular situation which makes you want to object to processing on this ground.

- Object to direct marketing where we are processing your personal information for direct marketing purposes. This is an absolute right, although not relevant to our CCTV and Access Control systems.

- Request the restriction of processing of your personal information. This enables you to ask us to stop processing your personal information for a period if it is inaccurate or there is a dispute about whether or not your interests override our legitimate grounds for processing your personal information.

- Request the transfer of your personal information to another party in certain circumstances.

- Object to certain automated decision making processes using your personal information.

You should note that some of these rights, for example the right to require us to transfer your personal information to another service provider or the right to object to automated decision making, may not apply as they have specific requirements and exemptions which apply to them and they may not apply to personal information recorded and stored by us. Also some of the rights will not apply to personal information in our CCTV and Access Control systems, for example we do not rely on consent in most cases and the personal information is not used for marketing, so whilst your right to withdraw your consent or object to processing for direct marketing are absolute rights, they will not be relevant to the personal information in our CCTV and Access Control systems. Also we do not use automated decision making which has legal or other significant effects for you in relation to your personal information in our CCTV and Access Control systems.

If you would like to exercise any of these rights, please contact our DPO at dpo@gymshark.com.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person or dealt with by a person who has no right to do so. We may also need you to provide details of specific times, dates and locations to allow us to locate any relevant personal information relating to you.

Whilst this privacy notice sets out a general summary of your legal rights in respect of personal information, this is a complex area of law. More information about your legal rights can be found on the ICO’s website at https://ico.org.uk/for-the-public/.

COMPLAINTS

We hope you don’t have any reason to complain, and we will always try to resolve any issues you have, but you always have the right to make a complaint at any time to the ICO about how we deal with your personal information or your rights in relation to your personal information. If you are based outside of the UK you may have the right to complain to your local data protection regulator.

You can make a compliant in writing to the ICO, Wycliffe House, Water Lane, Wilmslow, SK9 5AF, United Kingdom or you can go to https://ico.org.uk/make-a-complaint/.

CONTACTING US

If you have any queries regarding our use of your personal information or this privacy notice then please contact our DPO at dpo@gymshark.com or write to DPO, Gymshark, GSHQ, Blythe Valley Park, 3 Central boulevard, Solihull, B90 8AB, United Kingdom. You can use these details regardless of which of our group companies is the controller of your personal information in our CCTV and Access Control systems.

Dated: September 2020