Privacy Notice

TARMAC HOLDINGS LIMITED (Company Registration No. 7533961) and its group companies ("We"/"Our"/"Us") are committed to protecting and respecting your privacy.

This notice sets out the basis on which any personal data that we collect from you, or that you provide to us, will be processed by us. Please read the following carefully to understand our views and practices regarding your personal information and how we will treat it.

For the purposes of the General Data Protection Regulation (GDPR (EU) 2016/679), the Data Protection Act 2018 and any successor legislation ("data protection legislation"), we are the data controller for the data:

1.   about you which you provide in connection with the purpose below;
2.   which we or you enter into the system in this regard (or where this is otherwise entered into the system on your behalf);
3.   about your use of the system and our website; and
4.   in any correspondence we enter into with you.

CONTACT DETAILS
Our Contact Details: OneCard@tarmac.com
Questions, comments and requests regarding this privacy notice should be sent to DataProtection@tarmac.com.

PURPOSE
Our workforce (whether directly employed or subcontracted) participates in a workforce management card scheme called SkillGuard which provides real time authority to work for health and safety purposes for operatives and management. This comprises a database of individual records ("Worker Records"), associated smartcards enrolled on to that database and mobile apps which an individual who is checking the card ("card checker") may download onto a smartphone or tablet to access key data about cardholders on site to ensure they have the appropriate pre-requisites to work.

This workforce management card scheme also allows us to retain historic data in order to assist in the investigation of past incidents e.g. to ascertain if a worker was on site and the competencies held by the worker at the time of an incident.

Your personal data is processed for the purpose of participating in this card scheme and to enable your Employer and their administrator users, card checkers and, in certain circumstances, parties who are "Associated" to your Worker Record, to view your current competences, training and qualifications.

Data relating to administrators is also stored and processed to ensure relevant controls are in place so that access to workforce data can be restricted to only those individuals (administrators/authorised users) with a legitimate need to view/process this data, and so that an audit history of changes to data made by administrators can be maintained.

The ability of an administrator user to access your personal data varies according to the user role assigned to that individual. These users are authorised users of the system and may work on behalf of entities other than ourselves or your Employer organisation. They may be able to access your personal data (depending on the user role assigned to them) if you are or become unemployed because this allows you to be identified and assigned to a work project.

Your details may be updated or removed and further information about qualifications you hold may be electronically added to the chip in your card after your card has been issued. Your card may be cancelled at our discretion.

INFORMATION COLLECTED FROM YOU

Information that is stored in the database:

We may collect and store the following information in the database:

The cardholder's name, photograph, date of birth, alternative unique identifier e.g. national insurance number, postal address, phone number, e-mail address, emergency contact information, qualifications, competences, job roles, employment history, sponsorship status, data concerning health including medical examination date, medical provider, result of medical examination (satisfactory/unsatisfactory), D&A test result (pass/fail) and whether pre-appointment, periodic or for cause. Work restrictions, other information relevant to keeping the workforce safe on site. Formally delivered training and site-based events attended by the cardholder. Suspensions. The dates, times and locations where a card was swiped in or out. Linked Schemes and card numbers of other cards held by the cardholder in other card schemes.

We also collect and store personal data comprising the name and e-mail address of individuals granted access to the system as authorised users/administrators to allow them to be identified for user maintenance and audit purposes and their current Employer to allow their access to workforce data to be appropriately restricted.

Information that is collected and stored on the device (smartphone or tablet) used by a card checker to read your card:

Information that can be read from the card including: the cardholder's name, photograph, job roles, competences, training and qualifications as held on their Worker Record.

The dates and times when the card was read or swiped in/out and the last time the card was updated in the database.

You may view the information that is collected about you via mySkillGuard including the details of any other card schemes (Linked Schemes) with which your data is shared.

RECIPIENTS OR CATEGORIES OF RECIPIENT OF YOUR INFORMATION

We will share your personal information with third parties in the course of fulfilling the purpose for which we collected the information, including those purposes identified in this notice. We may disclose your personal information for a purpose directly related to these purposes that you would reasonably expect. We may also disclose your personal information where required for legal or safety reasons.

For example, we will share your personal data with:

- our services provider and data processor: Reference Point Limited (and it's sub processors) which provides us with services including hosting and online access to the SkillGuard database for our use in creating/registering and maintaining your Worker Record (and for the use of our contractors and sub-contractors) in relation to our business operations.
- the Vircarda service (operated by Reference Point Limited): if a virtual card is requested, its creation and updating will involve your personal data being copied from SkillGuard to your Vircarda digital wallet via the Vircarda backend service but personal data is not stored in the Vircarda backend service.
- any person checking your card using the mobile app: when your card is read electronically, a copy of your card is recorded together with other information held such as job roles, qualifications and competences. Where available, the time and location of checking and the last time the card was updated in the database are also recorded. This results in a log of the cards that have been read by the person reading your card.
- Linked Schemes: we may share your recent swipe in / out data (including travel time to/from place of rest) with other card schemes in circumstances where we have entered into a data sharing agreement to do so with another card scheme (a Linked Scheme) and that other card scheme's card number is included in your Worker Record. This allows your most recent swipe in / out data to be surfaced to card checkers upon the presentation of the card you hold for that other card scheme. The card checker may use this information to ascertain the hours you have recently worked in deciding on whether or not to allow you access to a work site (for health and safety purposes). You can view any Linked Schemes in mySkillGuard.
- parties benefiting from a SkillGuard API; this allows authorised third party systems to create Worker Records, update existing Worker Records, employ/unemploy a Worker and update Worker details. Worker Records may only be updated upon the input of the SkillGuard unique identifiers for that record. Your personal data will thus potentially be transferred from SkillGuard to a third party system.
- parties who are "Associated" to your Worker Record: depending on the user role assigned to them, we may share your personal information with administrator users and "Employers" or other members/registrants who are "Associated" to your Worker Record and who are authorised to use the system. They will thus be able to view your Worker Record, download it, print it and run reports including it if they input your unique reference number together with certain other key information which identifies you into the "Admin" menu on our site.
- third party payment providers: if we take a payment from you, we may pass your personal data to a third party payment provider, in particular where non corporate payment cards are used.

We may also disclose your personal information in order to comply with any legal obligation. This includes exchanging information with other companies and organisations for the purposes of fraud protection.

WHERE WE STORE YOUR PERSONAL INFORMATION AND TRANSFERS OUT OF THE EEA

The personal data that we collect from you will be stored within the UK and will be processed by staff operating within the UK who work for us or for one of our suppliers. We will not transfer any personal data that we collect or receive from you that constitutes personal data outside of the UK and the EEA unless there are appropriate safeguards or an adequacy decision in relation to the transfer as set out in the data protection legislation or the transfer otherwise complies with the data protection legislation. Such transfers may involve, for example, our use of third party services allowing us to send e-mails or automated SMS messages which make use of facilities in third countries to process and store data.

SECURITY
We will take all steps reasonably necessary to ensure that personal data you give us is treated securely and in accordance with this privacy policy.
To ensure data can only be accessed by the SkillGuard mobile app, all cardholder and swipe data is securely encrypted prior to being stored on the device. The cardholder data is encrypted on the device and cannot be read by anything other than the SkillGuard mobile app.
All information you provide to us is stored on our service provider's secure servers. Where we have given you (or where you have chosen) a password which enables you to access certain parts of our system, you are responsible for keeping this password confidential. We take steps to protect the information that we receive from you from loss, misuse, and unauthorised access or disclosure. These steps take into account the sensitivity of the information we receive, process and store, and the current state of technology. Our employees, contractors and service providers who provide services related to our information systems, are obliged to respect the confidentiality of any personal information held by us.

RETENTION PERIOD
We will delete personal data or de-identify (anonymise) it once sufficient time has elapsed to be certain it will no longer be required for those purposes for which it may be used under this policy. This will be 7 years from the time at which your Worker Record becomes "dormant" meaning from the time at which it was last edited or otherwise processed (save for deletion or storage).
Encrypted back ups: Our service provider will also retain encrypted back up tapes for a maximum of 3 years from the termination of our contract with it or from when we cease to use their services.

YOUR RIGHTS
If any of your information is out of date and you need to update it, please inform your Employer.
You have the right to find out what information we hold about you or to request a copy. If you wish to make such an access request you should contact DataProtection@tarmac.com. Our site may, from time to time, contain links to and from the websites of our partner

networks, advertisers and affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

COMPLAINTS TO INFORMATION COMMISSIONER
You have the right to lodge a complaint about our processing with the Information Commissioner.

CHANGES TO OUR PRIVACY POLICY
Any changes we may make to our privacy policy in the future will be posted on the relevant page on our site and, where appropriate, notified to you by e-mail. However, we advise that you check on our site regularly to keep up to date with any necessary changes. The current version of our privacy policy replaces all previous versions of the policy.

COOKIE POLICY
What are cookies?
Our website uses cookies to distinguish you from other users of our website. This helps us to provide you with a good experience when you browse our website and allows us to improve our site.
A cookie is a small file of letters and numbers that we store on your browser or the hard drive of your computer (or internet-enabled device) if you agree.
Cookies allow us to identify the computer or device you are using to access our website – but we cannot identify you personally. This information is sent back to our systems as you move around our website. Cookies are unique to the web browser you are using – so if you are using a desktop computer as well as a smart phone, different data will be collected for each.
Cookies we use
We use the following cookies:
Strictly necessary cookies: These are cookies that are required for the operation of our website. They include, for example, cookies that enable you to log into secure areas of our website and services.
Analytical/performance cookies: These allow us to recognise and count the number of visitors and to see how visitors move around our site when they are using it e.g. which pages are viewed by visitors most frequently. This helps us to improve the way our website and services work, for example, by ensuring that users are finding what they are looking for easily.
Functionality cookies. These are used to recognise you when you return to our site. This enables us to personalise our content for you and remember your preferences (for example, your choice of language or region).
We do not set targeting/advertising cookies. Cookies are not used in any Apps we provide.
Who sets cookies?
Cookies can be set by the owner of the website you are on. These are known as first party

cookies. Please note that third parties may also set cookies of any type, over which we have no control – however, you can control them by managing your cookies (see below). Only the owner of the cookie can see the anonymous information it collects.

How can I manage cookies?

You may block cookies by activating the setting on your browser which allows you to refuse the setting of all or some cookies. However, if you select this setting you may be unable to access all or certain parts of our site.

You can find more information about cookies on the ICO Website ico.org.uk/global/cookies and you can find detailed information on how you can control cookies at AboutCookies.org

We may need to update this Cookie Policy in the future and so encourage you to review this Cookie Policy periodically to stay informed about how we are using cookies. This Cookie Policy was last updated in February 2020.

If you have any questions or comments regarding our use of cookies, please e-mail OneCard@tarmac.com.