Security & Privacy Policy

This policy (Pol)019 is a key component of Totus' management framework and structure. It sets the requirements and responsibilities for maintaining the security of information within Totus. This policy may be supported by other policies and by guidance documents to assist putting the policy into practice day-to-day.

We are a 'controller' for the purposes of the General Data Protection Regulation (EU) 2016/679 ("Data Protection Laws").

We take your privacy 'very seriously'. We ask that you read this Security and Privacy Policy carefully as it contains important information about our processing and your rights.

In this document the term 'personal data' covers the data held in both computerised systems and contained within structured manual records.

General Data Protection Regulation (GDPR) 2016/679

The GDPR covers any information that relates to living individuals processed automatically or forms part of our administration filing systems and becomes an accessible record.

The processing of personal information includes obtaining, disclosing, recording, holding, using, erasing or destroying personal data.

Aim and Scope of this policy

The aim of this policy is to set out the rules governing the secure management of our personal data by:

- preserving the confidentiality, integrity and availability of our personal data.
- ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies
- Data must be processed lawfully, fairly and in a transparent manner in relation to individuals.
- Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

These principles must be followed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, Totus shall:

- observe fully the conditions regarding the fair collection and use of information including the giving of consent

- meet its legal obligations to specify the purposes for which information is used
- collect and process appropriate information only to the extent that it is needed to fulfil our operational needs or to comply with any legal requirements
- ensure the quality of information used
- ensure that the information is held for no longer than is necessary
- ensure that the rights of people about whom information is held can be fully exercised under the GDPR (i.e. the right to be informed that processing is being undertaken, to access one's personal information; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as incorrect)
- take appropriate technical and organisational security measures to safeguard personal information
- publicise and abide by individuals' right to appeal or complain to the supervisory authority (the Information Commissioner's Office (ICO)) in the event that agreement cannot be reached in a dispute regarding data protection
- ensure that personal information is not transferred abroad without suitable safeguards.

Responsibilities

- Ultimate responsibility for information security rests with Tim Read, HR Director of Totus, but on a day-to-day basis Sarah Woodward shall be responsible for managing and implementing the policy and related procedures.
- Line Managers are responsible for ensuring that their permanent staff, temporary staff and sub-contractors are aware of:-
  - The security and privacy policy and other relevant policies applicable in their work areas
  - Their personal responsibilities for information security
- All staff shall comply with the Security and Privacy Policy and must understand their duties and responsibilities to protect the company's data. Failure to do so may result in disciplinary action.
- Line managers shall be individually responsible for the security of information within their business area.
- Each member of staff shall be responsible for the operational security of the information systems they use.
- Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the personal data information they use is maintained to the highest standard.
- Access to the organisation's information systems by external parties shall only be allowed where a contract that requires compliance with this information security policy is in place. Such contracts shall require that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

Personnel Security

Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a security and confidentiality clause.
- References for new staff shall be verified and a passport, driving license or other document shall be provided to confirm identity and citizenship.
- Information security expectations of staff shall be included within appropriate job definitions.

- Whenever a staff member leaves the company their IT accounts will be disabled the same day they leave.

What Personal Data Do We Collect And Why?

Website Visitors Only

If you are just browsing our website we will not collect personal data, other than your IP address collected through our cookies. We will collect information about your usage of our website through cookies.
This information is statistical and aggregated and is not processed for the purpose of understanding your particular usage of the website. We collect this information so that we can:

- usage to improve its content, layout and performance;
- improve our tailor and personalise user experience;
- monitor our website services and products;

Information You Submit

We process personal information about you such as your name, address, email address and telephone number and anything else that you provide us. This information is obtained when you contact us by filling in a starter form, application form, contact form, complaints form, or placing an order for works. We do this in order to respond to the enquiry or complaint you are making.

We also collect personal information when you contact us directly via phone, email or in person; send us feedback or complete surveys which we use to improve our services and products in the future.

Marketing Emails

We do not send marketing emails.

Sensitive Personal Data Provided by You

We do not collect any sensitive personal data about you.

Personal Information About Other Individuals

If you give us information on behalf of someone else, you confirm that the other person has appointed you to act on their behalf and has agreed that you can.

How Is Processing Your Personal Data Lawful?

We are allowed to process your personal data on the basis that it is in our legitimate interests to:

- Monitor how our website is used in order to improve it. We use aggregated data to do this so it does not impact on your privacy;
- Respond to enquiries, complaints and requests in order to serve our customers. We will only use your personal data for this purpose. If you are an existing customer, we may add information about the enquiry, complaint or request to other records we hold about you so we can provide a better customer service;
- Respond to your request to purchase, so that we can fulfil your order,

- Send you materials you have requested, using the data you have provided.

Please be aware that you have the right to object to the processing of your data of any of the legitimate interests identified.

Who Will Have Access To Your Personal Data?

Like any business, we use service providers to operate our website, such as website hosting. We take steps to ensure that our service providers treat your data in accordance with the law, only use it in accordance with our contract with them and keep it secure.

Only those members of staff who require access to your personal data to fulfil the above requirements are given access.

How We Keep Your Data Secure

We strive to implement appropriate technical and organisational measures in order to protect your personal data against accidental or unlawful destruction, accidental loss or alteration, unauthorised disclosure or access and any other unlawful forms of processing. We aim to ensure that the level of security and the measures adopted to protect your personal data are appropriate for the risks presented by the nature and use of your personal data. We follow recognised industry practices for protecting our IT environment and physical facilities.

All staff are responsible for ensuring that:
- any personal data that they hold is kept securely
- personal information is not disclosed either orally or in writing or via Web

When Will We Delete Your Data?

Totus will not hold personal data for longer than necessary (excluding finance records where applicable) from the date when an employee/customer/supplier ceases their relationship with Totus. Personnel HR records will be kept for six years unless there is a business justification as why we need to keep for longer. Any unnecessary confidential information will be deleted immediately such as next of kin details and previous addresses etc.

Your Rights

As a data subject, you have the following legal rights:
- the right of access to personal data relating to you
- the right to correct any mistakes in your information
- the right to ask us to stop contacting you with direct marketing
- the right to prevent your personal data being processed in some circumstances
- the right to object to processing of your data where processed on the grounds of legitimate interests
- the right to erasure in some circumstances

If you would like to exercise your rights, please contact us at the details set out below.

We will respond to any rights that you exercise within a month of receiving your request, unless the request is particularly complex, in which case we will respond within three months.

Please note that exceptions apply to some of these rights which we will apply in accordance with the law.

How To Contact Us Regarding Our Security and Privacy Policy

If you have any questions about this policy, how we handle your personal data, or want to exercise any of your rights, please contact:

- Contact: Sarah Woodward
- Address: Totus Engineering Ltd, 10 Alder Court, Bell Close, Newnham Industrial Estate, Plympton, Plymouth, PL7 4JH
- Phone: +44 1752 295867
- Email: sarah.woodward@totus.co.uk

Complaints To The Regulator

If you do not think that we have processed your data in accordance with this policy, you should let us know as soon as possible. You also have the right to complain to the Information Commissioner's Office. Information about how to do this is available at www.ico.org.uk

Tim Read

Last Reviewed May 2023