TSG
BUILDING SERVICES plc

Data Protection & ICT Use Policy

TSG BUILDING SERVICES plc	**IMS Document Title**: Data Protection & ICT Use Policy		
	Department: IT	**Ref No**: IMS-PO-010	**ISO**: 9001 & 14001
	Approved By: Adam Thrussell	**Issue**: 2.0	**Date**: Jan 26

Data Protection & ICT Use Policy Statement

TSG takes its responsibilities with regard to the management of requirements of General Data Protection Regulation (GDPR) very seriously. This policy sets out how much the company manages those responsibilities.

TSG obtains, uses, stores and otherwise processes personal data relating to staff, current and former workers, contractors, clients, residents, website users and contacts, collectively referred to in this policy as data subjects. When processing personal data, TSG are obliged to fulfil individuals' reasonable expectations of privacy by complying with GDPR and other relevant data protection legislation (Data Protection Law).

This policy therefore seeks to ensure that we:

- Are clear about how personal data must be processed and TSG's expectations for all those who process personal data on its behalf;
- Comply with the Data Protection Law and with good practice.
- Protect TSG's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights.
- Protect TSG from risks of personal data breaches and other breaches of data protection law.

We recognise that information is fundamental to our successful operation and must be protected against breaches of confidentiality, failures of integrity and interruptions to availability. Effective information security is a combination of physical and technical security, together with appropriate policies which define the requirements which must be adhered to in order to safeguard information.

Signed:  **Date:** 2nd January 2026

Position: Chief Executive Officer & Owner

Data Protection & ICT Use Policy Statement

Introduction

TSG Building Services Plc is committed to ensuring that its data and ICT systems and processes are Compliant with all applicable legislative and regulatory requirements, including the Data Protection Act 1998 and the General Data Protection Regulation 2018 (GDPR). REGULATION (EU) 2016/679.

This policy meets the requirements of the former Data Protection act and the provisions of the GDPR and DPA from 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of personal information.

DPO (Data Protection Officer)

The DPO is responsible for monitoring and reviewing this policy, providing advice of our obligations under GDPR, cooperating with the ICO and acting as a point of contact with the ICO.

The DPO is also responsible for:

Providing DPIA (Data Protection Impact Assessments) where requested and taking into account the nature, scope, context and purposes of processing.

Policy Rights

We reserve the right to change this policy at any time without notice.

1. Policy Aims

1.1 The purpose of this policy is to provide guidance to Staff, Clients, Customers and Suppliers to TSG Building Services Plc and also contains our ICT Policy.

1.2. This policy supports the aim of TSG Building Services Plc to prioritise safeguarding and to provide a safe working environment for all employees.

1.3. This policy does not form part of the formal contract of employment for employees, but it is a condition of employment that employees abide by the rules and policies made by us whilst undertaking work for us or working directly for us an employee or providing services to us.

1.4. Any failures to follow this policy can therefore result in disciplinary proceedings for directly employed staff or grievance against third party service providers.

1.5. Any member of directly employed staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with their Line Manager initially.

1.6. If the matter is not resolved it should be raised as a formal grievance and brought to the attention of the Head of I.T and Data Protection Officer.

2. DPO & ICT

2.1. The Data Protection Officer is also responsible for ensuring the security of Information Communication Systems Technology.

2.2. All members of staff must be inducted by the IT Management before using TSG Building Services Plc's ICT systems. Guests are allowed use of TSG Building Services Plc's wireless service for the purpose of work related internet access only and must be issued with a temporary account (or their device registered with the IT department) in order of joining the Guest Wi-Fi.

3. Security and Use of ICT Systems

COMPANY COMPUTERS

3.1. The following measures will be undertaken by the IT department to ensure that our computers are secure:

(a) All computers will be protected by a firewall and antivirus software and all security updates and patches will be applied.

(b) Regular backups will be taken and kept in a secure place.

(c) Staff will only be allowed access to the information that they need to carry out their jobs.

(d) All data will be securely removed or destroyed from a TSGPLC computer when it is decommissioned.

(e) TSGPLC laptops that are issued to members of staff and may contain company data will be encrypted.

(f) Secure password policies will be enforced on staff and management accounts. Passwords will automatically expire after 3 months.

3.2. The contents of TSGPLC IT resources and communications systems are the property of TSG Building Services Plc. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communication systems except under the conditions laid out in in this Policy.

3.3. Staff are not permitted to use personal devices on TSG Building Services Plc network. Logs of user internet activity are recorded and will be kept private except under the conditions laid out in this Policy.

3.4. Staff are permitted to use the telephones for personal use only for emergencies such as contacting next of kin in a personal crisis. Messages and call logs will be kept private except under the conditions laid out in this Policy. A log of all users' activity on TSGPLC's network will be held for a reasonable time period. This information will be kept private unless requested for an appropriate reason, examples might include but are not limited to:

(a) Establishing the existence of facts.

(b) Ascertaining compliance with regulatory or self-regulatory procedures.

(c) Monitoring standards which are achieved by persons using our computers, telephony (except for telephones provided in staff accommodation) or hosted communication platforms (such as email and intranet) in the course of their duties and for staff training purposes.

(d) Prevention or detection of crime.

(e) To investigate or detect unauthorised use of TSGPLC's telecommunication system.

(f) To ensure the effective operation of the system such as protecting against viruses, backing up and making routine interceptions such as forwarding emails to the correct destination.

(g) For access to routine business communications, for instance checking voicemail and email when staff are on holiday or on sick leave.

3.6 Staff must adhere to the following guidelines:

(a) All passwords should be secure and never shared.

(b) USB memory sticks or other removable media (including CDs or DVDs should never be used to carry TSGPLC's data unless they are encrypted

(c) Only the minimum amount of data that is required to carry out your work should be copied to removable media such as USB memory sticks (encrypted).

(d) Computers should only be used by staff under close management supervision.

(e) Never leave a laptop or digital device on show in a car or unattended in a public space.

(f) Always make confidential phone calls in a private space and never in public (such as on a train).

(h) Paper records should be kept in accordance with your departments determined retention policy and should never be kept for longer than necessary (as detailed in Section 14).

(i) Paper documents containing personal or confidential information should be disposed of using TSG Building Services Plc's shredding service via the provided confidentiality bags.

EMAIL AND INTERNET USE

3.7. The following procedures will be adhered to by all staff when using TSG Building Services Plc email system:

(a) The use of a personal email account for TSG Building Services Plc business is prohibited.

(b) When sending email to multiple external recipients the bcc field must not be used inappropriately.

(c) TSG Building Services Plc email system must only be accessed from a Domain Registered computer.

(d) Appreciate that electronic mail is relatively insecure and consider security needs and confidentiality before transmission.

(e) No one except the named individual should have access to their company email account, except during an identified period, such as during absence, when they will alert all people who use this account that it is being managed by someone else.

(f) Any emails that are suspected to be fraudulent or "Phishing" should be reported to the IT Support team immediately.

3.8. Staff using TSG Building Services Plc's email or internet service must not:

(a) Create, transmit or cause to be transmitted material which is designed or likely to cause annoyance, inconvenience, needless anxiety or offence, and must not create, transmit or cause to be transmitted offensive obscene or indecent material.

(b) Create, transmit or cause to be transmitted defamatory material.

(c) Create, transmit or cause to be transmitted material such that the copyright of another person or party is infringed.

(d) Transmit by email any confidential information of TSG Building Services Plc otherwise than in the normal course of your duties.

(e) Send any message internally or externally which is abusive, humiliating, hostile or intimidating.

CLOUD STORAGE

3.9 The following procedures will be adhered to by all staff when using cloud based storage:

(a) The use of personal cloud storage solutions (such as, but not limited to Dropbox, Google Drive and OneDrive) for storage of any TSGPLC data is prohibited (unless expressly permitted in writing by the Head of IT).

(b) Staff wishing to use cloud based storage must utilise TSG Building Services Plc's cloud subscriptions only.

DEVICES

3.10. At all times Staff must minimize the amount of data that is held on personal devices and use the company devices we have provided them for the nature of their work.

3.11. All company devices must be secured with a strong password (i.e. contain a mix of upper and lower case characters, numbers and punctuation and be at least 10 characters in length)

3.12. All company devices must be configured to automatically lock after a short period of inactivity.

3.13. TSG Building Services Plc files or data must never be stored on a shared device.

3.14. If a mobile or tablet device becomes disfunctional, TSG Building Services Plc will, at its sole discretion, allow limited access to email via webmail or using the 'Microsoft OWA' app for an interim period.

3.15. Any device connected to TSG Building Services Plc's email system will be forced to enable a lock code and remote wipe facility.

3.16. Personal information must not be stored on a Company device unless in an emergency such as accidental loss or theft of a personal device.

3.17. Email and intranet access is strictly prohibited on a shared computer unless the account/profile is secured to the individual member of staff.

3.18. Company devices have a remote locate and wipe facility and by default all staff enter into agreement to enable this facility for security reasons.

PUBLIC WI-FI AND LANS

3.19. Any member of staff using a personal device for TSG Building Services Plc business on a public Wi-Fi connection will adhere to the following procedures:

(a) You will only use a public Wi-Fi connection from a trusted source (for example a Hotel service).

(b) Where applicable, devices must have a firewall enabled and file sharing turned off.

(c) You will take extra care to verify that the sites you are visiting are genuine and secure.

(d) When using a laptop or desktop computer you default to using TSGPLC's VPN system.

STORAGE AND USE OF DATA WITHIN TSG BUILDING SERVICES PLC'S DATA REPOSITORIES

3.22. All staff will adhere to the following procedures when working with data held within onsite Servers and Cloud based systems:

(a) All data (including email and calendars) will be secured so that only appropriate individuals will have access to it (the IT Support department can assist with configuring sharing preferences with specific permissions).

(b) Data intended for management only will not be stored in areas used for staff access.

(c) All TSG Building Services Plc devices or personal devices containing Company information should be digitally locked when left unattended when not in use in the office.

(d) Devices containing Company information should never be left unattended and/or unlocked when not in use in the office.

FORBIDDEN ICT ACTIVITIES

3.23. The consequences of undertaking any of the forbidden ICT activities listed below (or other instances) will be determined through the normal disciplinary procedures. All such activities are considered to be serious and are likely to be viewed as misconduct. It is likely that undertaking a forbidden activity, or repeating an unacceptable activity, will be viewed as gross misconduct.

(a) Using another person's identity so as to appear to be someone else.

(b) Attempting to gain or facilitate unauthorised access to a computer system or information.

(c) Attempting to or deliberately corrupting, destroying or denying access to another user's e-mail, data files, information, ICT system or service.

(d) Deliberately altering, bypassing or circumventing TSGPLC's advice on how to protect, store, transmit, share and access sensitive information both company Data Management System and Client Systems.

(e) Deliberately accessing, viewing, receiving, downloading, sending or storing material:

- with pornographic, offensive, obscene or indecent content;
- related to criminal skills or terrorist activities;
- that promote or encourage discrimination, racism or intolerance;
- that facilitates illegal activity in the UK or the host country;
- that is illegal in the UK or the host country;
- that is defamatory, threatening, harassing, offensive or abusive;
- that will, or is likely to, bring the TSG Building Services or any of its Clients into disrepute;
- that is known to be infected with a virus, worm, Trojan or any form of malicious software or code;
- that infringes the privacy and data protection rights of individuals;
- that could endanger the health and safety of any other individual or Client

4. Personal Data

4.1. Personal data covers any information relating to an identified or identifiable natural person including both facts and opinions about an individual.

The following data may be collected, held and processed:-

FOR CUSTOMERS & CLIENTS

a) Any given names, surname and title

b) Address details for home and work with preferred contact address

c) Email address for receipt of email correspondence

d) Telephone numbers: work, home and mobile

e) Bank account details

f) Professional work details

FOR EMPLOYEES

a) Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses

b) Date of birth

c) Gender

d) Marital status and dependants

e) Next of kin and emergency contact information

f) National Insurance number

g) Bank account details, payroll records and tax status information

h) Salary, annual leave, pension and benefits information

i) Start date

j) Location of employment or workplace

k) Copy of driving licence / Passport / Identity Card

l) Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process.

m) Employment records (including job titles, work history, working hours, training records and professional memberships)

n) Remuneration history

o) Performance information

p) Disciplinary and grievance information

q) Proof of Disability

DISCLOSURE OF PERSONAL DATA

4.2. The data we process is to ensure vital interests of the individual e.g. to protect someone's life by carrying out essential Health and Safety related maintenance, repairs or servicing to a property and as contracted by the Client, Landlord, Housing Association or Council.

However, data may be disclosed to law enforcement (such as the police) and safeguarding agencies (such as the local authority) without consent in certain circumstances such as but not limited to the following examples:

(a) If a customer makes a complaint about a member of staff that the name of the person involved may be passed on to law enforcement and safeguarding agencies.

(b) Information in staff witness statements may be disclosed for purposes of addressing bullying or harassment allegations. Any sensitive personal data asides from names may be redacted.

(c) Where allegations have been made against a member of staff which are reported to staff/social services that the name of the person involved may be passed on to law enforcement and safeguarding agencies.

(d) Where it will ensure the safety of staff or other members of the public and members of Council, Landlord or Housing Association that the name of the person involved may be passed on to law enforcement and safeguarding agencies.

(e) If TSG Building Services Plc is required to do so by the law. (For safeguarding requirements) Names of relevant persons may be passed on to law enforcement and safeguarding agencies.

5. Sensitive Personal Data (Special Category Data)

5.1. TSG Building Services Plc may, from time to time, be required to process special categories of (sensitive) personal data regarding a worker, customer or Client. Sensitive personal data includes medical information, vulnerabilities, UDC's & Cautionaries. Data relating to age, religion, trade union membership and criminal records. Where sensitive personal data is processed by TSG Building Services Plc, the explicit consent of the worker, customer or Client will generally be required in writing. However, in certain circumstances it may be processed without consent such as where it is required to protect the vital interests of an individual, it is necessary in relation to a legal claim or in some employment contexts.

5.2. Any member of staff collecting or in any way working with personal data must do so in line with the GDPR principles:

(a) Lawfulness, fairness and transparency

(b) Purpose limitation

(c) Data minimisation

(d) Accuracy

(e) Storage limitation

(f) Integrity and confidentiality (security)

(g) Accountability

All Department Heads are required (though the use of TSG Building Services Plc's established data management framework.) to:-

(h) Map all data in use and identify any data processing in use that is likely to result in a high risk to individuals.

(g) Carry out a data protection impact assessment (DPIA) on any data processing in use that is likely to result in a high risk to individuals.

The DPIA process will:

(i) Describe how the information within a data processing operation is collected, stored, used and deleted.

(j) Identify privacy and related risks – catalogue the range of threats, and their related vulnerabilities, to the rights and freedoms of individuals whose data is collected and/or processed.

(k) Identify and evaluate privacy solutions – for each identified risk to the personal data, make a 'risk decision', i.e. whether to accept or reject the risk, whether to transfer it or take steps to reduce the impact or likelihood of the threat successfully exploiting the vulnerability.

TSG Building Services Plc's Senior Team will be responsible for approving suggested DPIA outcomes and risk management strategies.

6. Photography & Geolocation

6.1. When dealing with photography, staff and management must adhere to the following guidelines:

(a) When taking photographs/video for official work purposes/as part of contractual data or for publication to TSG Building Services Plc website/portal (or Client's Website) the subjects must be informed of the intended use and the photographs/video used only for that purpose. It is sufficient to provide this as verbal communication prior to photo taking.

(b) Staff or Management must never take pictures of customers using either their company or personal camera or mobile device unless they have been given permission to do so as part of an agreed case study, agreed with all relevant parties.

(c) Photographs should be deleted when the original purpose is no longer valid.

(d) Photographs/video within an individual's property should never be uploaded to any third party website / social media site.

(e) Geo-location must never reveal the personal address and/or full identity of any worker to any member of the public via any TSGPLC internet communication systems.

7. Social Media

USE OF SOCIAL MEDIA FOR TSG BUILDING SERVICES PLC PURPOSES

7.1. The use of TSG Building Services Plc official social media platforms is encouraged for use by all staff, management, customers, clients, suppliers and providers.

(a) All TSGPLC Social Media accounts and their content is managed by our in-house marketing team with the Head of HR to deem all content appropriate before being published. We take into account that information/images published without permission may result in TSG Building Services Plc being prosecuted.

(b) A set of guidelines is established as to how and for what purpose the social media accounts may be used and this is overseen by the Head of HR.

(c) TSG Building Services Plc account is created with the social media provider only, and not any affiliates and is kept separate and secure from any personal accounts or other business accounts.

7.2. Staff and management must be aware that their role comes with particular responsibilities and they must adhere to TSG Building Services Plc's approach to social media use and:

(a) Ensure that no staff makes posts to our social media on the behalf of another member of staff

(b) Not upload any comments which could be deemed politically incorrect, offensive or abusive in any manner.

(c) Report to their Head of Department or Line Manager immediately if they see any information on the internet, intranet or on social networking sites that disparages or reflects poorly on TSG Building Services Plc.

(d) Immediately remove any internet postings which are deemed by TSG Building Services Plc to constitute a breach of this or any other TSG Building Services Plc policy. Staff who fail to remove such posts may be subject to disciplinary action.

(e) Consider whether a particular posting puts their effectiveness as an employee at risk.

(f) Post only what they want the world and other employees to see.

(g) Provide references for other individuals, on external social or professional networking sites, as such references whether positive or negative can be attributed to TSG Building Services Plc and create legal issues for both parties if an appeal is raised by the individual in question to the media site enquiries/report section.

(h) Post or publish on the internet or on any external social networking site, any false accusations regarding any of TSG Building Services Plc staff, supervisors or management.

(i) Not use commentary deemed to be defamatory, obscene, proprietary, or libellous. Staff must exercise caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterisations.

(j) Not post immaterial or offensive images.

(k) Not associate a TSGPLC email address with any external social media accounts.

7.5. TSG Building Services Plc recognises that workers may need to work long hours and occasionally may desire to use of their own social media accounts for personal activities at the office or by means of our computers, networks, company mobiles and other TSGPLC IT resources and communications systems. We authorise such occasional use in these circumstances so long as it does not involve unprofessional or inappropriate content, and does not interfere with employment responsibilities or productivity and otherwise complies with this policy.

While using personal social media at work in this overtime scenario; circulating chain letters or other spam is never permitted. Circulating or posting commercial, personal, religious or political solicitations, or promotion of outside organisations unrelated to or in competition with TSG Building Services Plc's business is also prohibited. Staff must ensure that their use of social media does not create any breaches of internet security and therefore must be careful to avoid any applications that might evoke our Internet Securities. Excessive use of social media that interrupts staff productivity and/or compromises the security of the company will be subject to a disciplinary procedure, consistent with this policy.

MONITORING OF SOCIAL MEDIA

7.6. In line our Employee Computer and Internet usage Policy, we reserve the right to monitor, intercept and review, without further notice, staff activities using TSGPLC's IT resources and communications systems, including but not limited to social media postings and internet activities, to ensure that our rules are being complied with and for legitimate business purposes. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses TSGPLC's network systems as well as inspection of Internet Log files.

SOCIAL MEDIA AND PERSNAL DATA AT THE END OF EMPLOYMENT

7.7. If a member of staff's employment with TSG Building Services Plc should end, for whatever reason, any reference to said worker on TSG's official social networking sites will be immediately amended to reflect the fact that they are no longer employed or associated with TSG Building Services Plc.

7.8. All professional contacts that a member of staff has made through their course of employment with TSG Building Services Plc belongs to the Company, regardless of whether or not the member of staff has made social media connections with them.

7.9. Exiting employees or any employee should note that ANY comment made in a TSG Building Services Plc email at any time can potentially be disclosed. There is NO EXEMPTION for 'embarrassing' comments made about another individual at any stage of employment.

7.10. Unless TSG Building Services Plc has reasonable grounds to refuse the erasure of personal data for an existing employee, all requests for erasure shall be complied with, and the data subject informed of the erasure within one month of receipt of the data subject's request (this can be extended by up to three months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

8. Lost Data

8.1. Security breaches must be reported to the Head of I.T and Data Protection Officer and dealt with immediately as per the Data Breach Procedures outlined in section 11 of this Policy.

8.2. Actions that must be carried out include:

(a) Devise a breach specific recover and damage limitation plan in line with the standard policy and procedures.

(b) Inform appropriate people and organisations.

(c) Review response and update information security.

9. Personal Data Requests

9.1. Requests to provide Personal Data should be emailed to dpo@tsgplc.co.uk with reasons to substantiate the need for the Data Access that is being requested.

9.2. Requests to erase Personal Data by the subject should be emailed to dpo@tsgplc.co.uk with reasons to substantiate the need for the erasure being requested.

9.3. These requests will follow a Personal Data request procedure.

SUBJECT ACCESS REQUEST

9.4. A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which TSG Building Services Plc hold about them and also request to exercise one or more of the Rights of Data Subjects.

In doing so we shall also act in accordance with the Rights of Data Subjects outlined in the GDPR. But not where the subject is the ownership of a Data Provider. For Example Tenant to a Landlord or Housing Association without first advising the Client of the tenants request to:

a) be informed of what their personal data is used for
b) access a copy their personal data that we store
c) rectification of their personal data that we store
d) have their personal data removed (be forgotten)
e) restrict or cease processing of personal their data
f) restrict or cease transference of their personal data
g) object to the use of their personal data
h) object to the automated decision-making and profiling of their personal data

10. Personal Data Overseas

10.1. No personal data should be taken overseas (outside of the EU) unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals when processing their personal data.

10.2. Any worker who plans to travel to a country outside of the EU with TSG Building Services Plc data must inform the DPO.

10.3. Any worker who intends to transfer TSG Building Services Plc data outside of the EU must inform the DPO.

11. Breach of Policy and Data Breach

11.1. Any breaches of this policy may result in disciplinary action, and for more serious breaches dismissal.

DATA BREACH NOTIFICATION

11.2. All personal data breaches must be reported immediately to the DPO.

11.3. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the DPO must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

11.4. In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 11.3 to the rights and freedoms of data subjects, the DPO must ensure that all affected data subjects are informed of the breach directly and without undue delay.

11.5. Data breach notifications shall include the following information:

a) The categories and approximate number of data subjects concerned;

b) The categories and approximate number of personal data records concerned;

c) The name and contact details of the DPO (or other contact point where more information can be obtained);

d) The likely consequences of the breach;

e) Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the ICO and using the guidelines endorsed by the European Data Protection Board for handling data breaches.

11.6. On finding a breach, the staff member or data processor must immediately notify the DPO.

11.7. The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

11.8. Lost, stolen, destroyed, altered, disclosed or made available where it should not have been
made available to unauthorised people.

11.9. The DPO will alert the Proprietor of the Company.

11.10. The DPO will make all reasonable efforts to contain and minimise the impact of the breach,
assisted by the Head of IT and any relevant staff members or data processors where necessary.

11.11. The DPO will assess the potential consequences, based on how serious they are, and how
likely they are to happen.

11.12. The DPO will work out whether the breach must be reported to the ICO. This must be judged
on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

(a) Loss of control of their data
(b) Discrimination
(c) Identity theft or fraud
(d) Financial less
(e) Unauthorised reversal of pseudonymisation (for example key-coding)
(f) Damage to reputation
(g) Loss of confidentiality
(h) Any other significant economic or social disadvantage to the individual(s) concerned

if it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

11.13. The DPO will document the decision (either way), in case it is challenged at a later date by
the ICO or an individual affected by the breach.

11.14. Documented decisions are stored on the Company network drive in a secure folder.

11.15. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the
ICO website within 72 hours. As required, the DPO will set out:

(a) A description of the nature of the personal data breach including, where possible:
(b) The categories and approximate number of individuals concerned
(c) The categories and approximate number of personal records concerned
(d) The name and contact details of the DPO
(e) A description of the likely consequences of the personal data breach
(f) A description of the measures that have been, or will be, taken to deal with the
(g) breach and mitigate any possible adverse effects on the individual(s) concerned

11.16. If all the above details are not yet known, the DPO will report as much as they can within 72
hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

11.17. The DPO will also assess the risk to individuals, again based on the severity and likelihood of
potential or actual impact.

11.18. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

(a) The name and contact details of the DPO
(b) A description of the likely consequences of the personal data breach
(c) A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

11.19. The DPO will notify any relevant third parties who can help mitigate the loss to individuals.\
For example: The police, insurers, banks or credit card companies.

11.20. The DPO will document each breach, irrespective of whether it is reported to the ICO. For
each breach, this record will include the: Facts and cause, the Effects, the action taken to contain it and ensure it does not happen again (such as establishing a more robust processes or providing further training for individuals).

11.21. Records of all breaches will be stored in a secure network folder.

11.22. The DPO and proprietor of the Company will meet to review what happened and how it can

Be stopped from happening again. This meeting will happen as soon as reasonably possible and shall the outcomes shall be documented in our Integrated Management Systems processes and procedures and where identifiable this policy updated.

12. Central Data Retention Periods

12.1. Correspondence to be destroyed after 10 years.

12.2. Digital financial records to be destroyed after 10 years.

12.3. Invoices and petty cash slips to be destroyed after 6 years.

12.4. Paper files to be destroyed after 7 years.

12.5. Correspondence and digital files to be destroyed after 10 years.

12.6 Paper and digital files containing personal data to be destroyed after 10 years.

13. Training

13.1. All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including Privacy and Security of the Internet or Things.

13.2. All staff members will receive refresher training at least once each year as part of safeguarding training, as well as relevant updates as required (for example through emails, bulletins
staff meetings and toolbox talks).

13.3. All staff will also update their GDPR Essential Skills knowledge and skills on the subject of online safety at regular intervals, and at least annually.

13.4. Proprietors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training and will also be sent to Data Protection awareness courses/seminars.

13.5. Data protection will also form part of continuing professional development, where changes to
Legislation, guidance or the processes make it necessary.

14. Third-Party Data Processors (Sub Contractors)

14.1. Where external companies are used to process personal data on our behalf, the responsibility for the security and appropriate use of that data remains with TSG Building Services Plc.

14.2. Where a third-party data processor is used, a contract which establishes what personal data will be processed and for what purpose; must be signed in agreement prior to engagement of any works with them.

14.3. Subcontractors will also receive appropriate training as part of their induction and receive updates as applicable.