Acceptable Use of IT Policy

Berg en Dal Homeowners Association

1. Introduction

"**IT**" is a combination of information, communications, and technology. This policy applies to the use of IT by all employees, contractors, agents, trustees, and committee members of the Berg en Dal Homeowners Association ("**HOA**").

This policy does not unreasonably limit your ability to use IT in your personal life. But, what you do in your personal capacity can reflect on us if someone can identify the professional relationship between us. So, this policy applies to your personal use of IT whenever you do anything that can be linked back to the HOA.

2. Acceptable standards

2.1 ***Use***. You may need to use IT for the acceptable purpose of doing HOA business in your capacity as an employee, contractor, agent, trustee, or committee member of the HOA. However, you may not:

- **Use HOA IT** to send inappropriate messages, chain emails, or spam. These communication tools should be utilised for official HOA business only and in accordance with our privacy policy;
- **Use your HOA email account** for excessive personal correspondence or to sign up for newsletters, or web services not related to your work.

2.2 ***Content***. You may not use HOA IT to publish:

- **illegal content** that is prohibited by law – like child pornography, pirated content, or content that otherwise infringes someone else's rights;
- **harmful content** that could cause harm to someone – like defamatory comments, fraudulent claims, or untrue statements;
- **offensive content** that could reasonably offend someone – like pornography, obscenities, or prejudicial or discriminatory statements; or
- **impermissible content** – contrary to any codes or standards that we subscribe to.

2.3 ***Responsibility***. You are responsible for anything that you do with IT in your personal capacity.

3. Information

3.1 ***Types***. You may handle various types of information during your relationship with us, including:

- **homeowner information** –including contact information, account information;
- **HOA business information** – including employee payroll, financials, meeting notes, meeting minutes, reports, CVs, and references;
- **confidential information** – that is only known to you through your relationship with us;
- **restricted information** – that should only be known to authorised persons and may not include you; and
- **illegal information** – that should not be known to anyone.

3.2 ***Access***. We give you access to all types of information that we collect or generate subject to certain restrictions, but it is your responsibility to protect it by:

- only using it for the purpose that we gave you access to it for;
- storing it appropriately and creating any necessary backups;
- only retaining it for as long as is necessary for that purpose;
- not disclosing it to anyone that you shouldn't be disclosing it to;
- ensuring that it is secure and not accessible to anyone who shouldn't have access to it.

3.3 ***Restrictions***. Each type of personal information is subject to the following restrictions:

- **homeowner information** – you must help us process this lawfully in terms of the relevant data protection laws;
- **HOA business information** – you must not disclose this to anyone outside of our organisation;
- **confidential information** – you may not disclose this to any person that we have not authorised to receive it.;
- **restricted information** – you may not obtain or use this unless you have the right to obtain or use it; and
- **illegal information** – you may not process this at all.

3.4 ***Breach***. We take information security very seriously and ask you to do the same, but security breaches can still happen. If there is a security breach or if you suspect there has been one, you must notify us by email as soon as possible. The notification must contain sufficient information for us to limit the consequences of the security breach, including a description of the possible consequences, a description of the measures you have taken to handle the breach, recommendations for how we can limit the consequences of the breach, and the identity of the unauthorised person if it is known to you.

4. Communication

4.1 ***Channels***. We may provide you with access to communication channels so that you can do business by communicating with our homeowners, employees, contractors, agents, trustees, and committee members.

4.2 ***Representation***. You will be representing us whenever you transmit something over a channel that could be associated with us. You may not represent us contrary to the acceptable standards clause of this policy.

4.3 ***Email***. If we provide you with an email address and want you to use it to do business, please be careful of the following risks:

- **identification** – make sure that your email identifies you to its recipient with your full name and not just your email address;
- **disclaimers** – ensure that your email contains all links to our relevant email disclaimers;
- **signatures** – be aware that an email from you to someone could constitute your electronic signature or consent if the contents of the message indicates a willingness to be bound, so be careful what you say in your emails;
- **unsolicited messages** – make sure that your messages aren't unsolicited or the recipient may consider them to be spam;

- **bulk sending** – Bcc (Blind carbon copy) is the only option when you want to send a message to lots of other people while protecting the identity of the other recipients, so make sure that you understand when you should and shouldn't use CC (Carbon copy);
- **printing** – paper is inefficient, it kills trees, and costs our organisation money, so please don't print unless you really need to;
- **contents** – please don't alter the contents of the original email when you forward it or reply unless absolutely necessary, in which case you should mark the changes clearly;
- **file size** – please don't send emails or attachments that are too large, because we may need to limit the size of incoming and outgoing emails and attachments and delete any that are too big to conserve bandwidth and for security reasons; and
- **deletions** – please don't delete any emails or attachments if there is any chance that the organisation may require them later.

4.4 ***Social media***. If you use social media to do business or in a way that could be connected to the HOA:

- **identification** – you must identify yourself with your name and role within the HOA whenever you publish anything that could be connected to us;
- **no agency** – you may not publish anything purporting to be our opinion or published on our behalf without our written permission;
- **representation** – the mere fact of our relationship does not imply that we have authorised you to speak as our representative;
- **confidentiality** – you must only publish content on social media that consists of publicly available information and does not disclose any confidential information that you only know because you work for us;
- **veracity** – you must only publish content on social media if it consists of true and accurate information;
- **compliance** – anything that you publish on social media must comply with the relevant social media service's legal terms and any relevant copyright and other laws;
- **removal** – you must remove anything that you have published on social media that can be linked back to us if we inform you in writing that it is contrary to this policy;
- **our intellectual property** – anything that you publish on social media may not contain your HOA email address, our logos, trademarks, or anything else that could make it look like we have endorsed what you have published, unless we have given you written permission to do so;
- **references** – you may not refer to our homeowners in anything that you post on social media without their permission; and
- **attribution** – you must also link back to the source of your statements whenever possible.

4.5 ***Account security***.

We may provide you with various credentials in the form of usernames and passwords to access HOA communication channel accounts. These credentials pose security risks to us if you don't look after them. There is no such thing as absolute security, but there are various steps you can take to improve security. For this reason, please take the following account security steps:

- **access controls** – please respect credentials and other access controls, because they are there to ensure that only authorised employees and contractors have access to our communications channels necessary to do their jobs;
- **password responsibility** – you are responsible for all transactions made under your credentials, even if someone obtained them without your permission;
- **password confidentiality** – your password is only for your use and you are not allowed to share it with anyone else;
- **password strength** – you must use a sufficiently strong password that it is difficult to guess;
- **password changes** – you must change your password immediately if you suspect that someone else knows it or otherwise from time to time to reduce the chances of someone else knowing it;
- **password management** – you must not store your password so that others can find it, for example on paper or in a file on your device.

5. Technology

5.1 ***Device protection***. If you are using personal devices to do HOA business, or if you are using any HOA IT infrastructure, you should:

- **password security** – not save any passwords or other credentials anywhere on the device, including taping notes to the device itself or keeping notes inside the carry case of the device;
- **data security** – make sure that the data and software stored on it is protected and secure.

5.2 ***Malicious software***. Malicious software includes programmes like viruses, trojan horses, and spyware that are meant to disrupt and damage IT. We need you to help us protect against these threats by:

- not introducing any malicious software to our IT equipment or infrastructure for any reason;
- activating antivirus software and updating it regularly;
- updating operating systems and other critical software with security and related patches regularly; and
- not running software from unknown or disreputable sources.

5.3 ***Prohibited insecure conduct***. You may not use IT equipment or infrastructure to do anything that would threaten our security or that of another system, including accessing or using any system without permission, or interfering with the proper functioning of any system.

6. General

6.1 ***Monitoring***. We will respect your right to privacy to greatest possible extent, but your right to privacy is limited in the interests of the business and we have the right to:

- monitor all internet traffic passing through our IT infrastructure;
- monitor any emails passing through our IT infrastructure; and
- access any file stored on our IT equipment or infrastructure;

provided that it is performed by our properly authorised representative for a lawful purpose strictly in accordance with any monitoring policy and procedures that we may have.

6.2 ***Blocking***. We may block and delete any information passing through our IT infrastructure. We also reserve the right to block any

type of information that is deemed not to be in the best interests of our business.

6.3 ***Liability***. We will not accept any liability for your use of IT when used for personal use, and you indemnify us against any liability. You need to clearly understand that your use of IT may cause us to be held legally liable.

6.4 ***Indemnity***. You indemnify us against any claims arising out of a breach of this policy.

6.5 ***Changes***. We may change the terms at any time and where this affects your rights and obligations, we will notify you of any changes by email.

6.6 ***Enquiries***. If you have any questions or concerns arising from this policy or the way in which we handle social media, please contact us.