

The Proximity Group Ltd.'s General Data Protection Act and Data Privacy Policy is to be used with The Proximity Group Ltd.'s Data Retention Policy to adhere to the UK GDPR and Data Protection Act of 2018.

The Privacy Policy consists of the following sections:

- Overview.
- Principles of Data Protection
- Defining how we use personal data.
- Define the categories of personal data.
- Define processing of data
- How will we process your personal data.
- Examples of when we might process your personal data.
- Sharing your personal data.
- How should you process personal data for the business?
- How to deal with data breaches.
- Subject access requests.
- Your data subject rights and the following Detailed Policies.
- Email, Internet Acceptable, Social-Media, Corporate Infrastructure, Business Application, Infrastructure Monitoring policies listed below.

Overview

("The Proximity Group Ltd") takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the UK GDPR and Data Protection Act of 2018 in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

This policy applies to all staff and consultants of The Proximity Group Ltd. You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to your data.

The Proximity Group Ltd has measures in place to protect the security of your data and retain it for no longer than is necessary. Our security systems include physical as well as computer security measures.

Your data is held for no longer than the law requires, and we follow CIPD guidelines on retention guidelines for employment personal data. We will only hold data for as long as necessary for the purposes for which we collected it.

The Proximity Group Ltd is a 'data controller' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

This policy explains how we will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing, or storing personal data while working for, or on behalf of, The Proximity Group Ltd. This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by us at any time. It is intended that this policy is fully compliant with the UK GDPR and Data Protection Act of 2018. If any conflict arises between those laws and this policy, we intend to comply with the UK GDPR and Data Protection Act of 2018.

Data Protection Principles

Personal data must be processed in accordance with seven 'Data Protection Principles.' It must:

- be processed fairly, lawfully, and transparently ('lawfulness, fairness and transparency').
- be collected and processed only for specified, explicit and legitimate purposes ('purpose limitation').
- be adequate, relevant, and limited to what is necessary for the purposes for which it is processed ('data minimisation').

- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay ('accuracy').
- not be kept for longer than is necessary for the purposes for which it is processed ('storage limitation').
- be processed securely ('integrity and confidentiality') and.
- As we are accountable for these principles and must be able to show that we are compliant ('accountability').

How we define personal data

'Personal data' means information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

We will collect and use the following types of personal data about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants/family details.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension, and benefits information.
- Start date and end date of employment.
- Information about your contract of employment.
- Location of employment or workplace.
- Copy of driving licence.
- Recruitment information (including copies of right to work documentation, references, qualifications and membership of any professional bodies and details of any preemployment assessments and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Compensation history.
- Information relating to your performance and behaviour at work.
- Information relating to disciplinary or grievance investigations and proceedings involving you (whether you were the main subject of those proceedings).
- Disciplinary and grievance information.
- Training and CPD records.
- CCTV footage and other information obtained through electronic means such as swipe card records.
- Information about your use of our information, telephone, alarm, and communications systems.
- Your images, whether in CCTV, by photograph or video.
- Any other category of personal data which we may notify you of from time to time.

How we define special categories of personal data

'Special categories of personal data' are types of personal data consisting of information as to information about:

- your race or ethnicity, religious or philosophical beliefs, sexual orientation, and political opinions.
- trade union membership.
- your health, including any medical condition, health, and sickness records.
- genetic information and biometric data; and
- criminal convictions and offences.

We may hold and use any of these special categories of your personal data in accordance with the law.

How we define processing

'Processing' means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring, or storage.
- adaption or alteration.
- Retrieval, consultation, or use.
- disclosure by transmission, dissemination or otherwise making available.
- alignment or combination; and
- restriction, destruction, or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

How will we process your personal data?

The Proximity Group Ltd will process your personal data (including special categories of personal data) in accordance with our obligations under the UK GDPR.

We will use your personal data for:

- performing the contract of employment (or services) between us.
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else).

However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights under data rights section.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain personal data, you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details, we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

Examples of when we might process your personal data.

We must process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

For example,

- to decide whether to employ (or engage) you.
- to decide how much to pay you, and the other terms of your contract with us.
- to administer the terms of your contract with us.
- to check you have the legal right to work for us/to work in the UK.
- to carry out the contract between us including where relevant, its termination.
- training you and reviewing your performance.

- to assess qualifications for a particular job or task, including decisions on whether to promote you.
- to decide whether and how to manage your performance, absence, or conduct.
- to make decisions about your continued employment or engagement.
- to plan for the termination of our working relationship.
- to gather evidence for or carry out a disciplinary or grievance investigation or procedure in relation to you or someone else.
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability.
- to monitor diversity and equal opportunities.
- to monitor and protect the security (including network security) of The Proximity Group Ltd, of you, us, or other staff, customers, and others.
- to monitor and protect the health and safety of you, our other staff, customers and third parties.
- to pay you and provide pension and other benefits in accordance with the contract between us and liaison with your pension provider or other providers of benefits.
- paying tax and national insurance.
- to provide a reference upon request from another employer.
- to monitor your use of our information and communication systems to ensure compliance with our IT policies.
- to ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- to monitor compliance by you, us and others with our policies and our contractual obligations.
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us.
- to conduct data analytics studies to review and better understand employee retention and attrition rates.
- equal opportunities monitoring.
- to answer questions from insurers in respect of any insurance policies which relate to You.
- running, managing, and planning our business, including but not limited to accounting and auditing.
- the prevention and detection of fraud or other criminal offences.
- to defend The Proximity Group Ltd in respect of any investigation, litigation, or accidents at work and to comply with any court or tribunal orders for disclosure; and
- for any other reason which we may notify you of from time to time.

We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data, then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting The Proximity Group Ltd's Director of Operations (Morne Brits).

We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law.
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent.
- where you have made the data public.
- where processing is necessary for the establishment, exercise, or defence of legal claims and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity, subject to appropriate confidentiality safeguards.

We might process special categories of your personal data for the purposes of the above listed categories, beside them. In particular, we will use information in relation to:

- your race, ethnic origin, religion, sexual orientation, or gender to monitor equal opportunities.
- leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws; and
- your sickness absence, health, and medical conditions to monitor and manage your absence, assess your fitness for work, to provide you with or pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety. We do not take automated decisions about you using your personal data or use profiling in relation to you.

Sharing your personal data

Sometimes we might share your personal data with pension and benefit providers, IT software, and hardware providers, alarm and security companies, legal directories, medical professionals, group companies or our contractors and agents, stakeholders, suppliers, and distributors to carry out our obligations under our contract with you or for our legitimate interests.

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

Third parties use your personal data to administer and process payroll, pension, and benefits, to provide our IT systems and services, to administer other services for the business and to assist us with carrying out our obligations under our contract with you.

We may also use outsourced services in countries outside the European Union from time to time in other aspects of our business.

Accordingly, data obtained within the UK, or any other country could be processed outside the European Union. For example, some of the software our website uses may have been developed in the United States of America or in Australia.

We use the following safeguards with respect to data transferred outside the European Union:

The data protection clauses in our contracts with data processors include transfer clauses written by or approved by a supervisory authority in the European Union.

How should one process personal data for the business?

Everyone who works for, or on behalf of, The Proximity Group Ltd has some responsibility for ensuring data is collected, stored, and handled appropriately.

The Proximity Group Ltd.'s Head of Operations at the time of issuing this policy is Morne Brits and is responsible for reviewing this policy. You should direct any questions in relation to this policy or data protection to this person. You must comply with all the Detailed Policies which follow in this Privacy Policy concerning your use of IT systems and which comprise:

- Email Acceptable Usage
- Internet Acceptable Usage
- Social Media Acceptable Use
- Corporate Infrastructure
- Business Application
- Infrastructure Monitoring

You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of The Proximity Group Ltd and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

You should not share personal data informally.

You should keep personal data secure and not share it with unauthorised people.

You should regularly review and update personal data which you must deal with for work.

This includes telling us if your own contact details change.

You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

You should use strong passwords.

You should lock your computer screens when not at your desk.

Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

Do not save personal data to your own personal computers or other devices.

Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Director of Operations.

You should lock drawers and filing cabinets.

Do not leave paper with personal data lying about.

You should not take personal data away from The Proximity Group Ltd.'s premises without authorisation from your line manager.

Personal data should be shredded and disposed of securely when you have finished with it.

You should ask for help from the Head of Compliance if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

Any breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure, and in sufficiently serious cases could be considered gross misconduct, which could result in your dismissal.

It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below).

This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

How to deal with data breaches

We have strict measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we must also notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach you must contact the Director of Operations immediately and keep any evidence, you have in relation to the breach. For further information, reach out to our Director of Operations for assistance.

Subject access requests

Data subjects can make a 'subject access request' ('SAR') to find out the information we hold about them. This request should be made in writing. If you receive such a request, you should forward it immediately to the Director of Operations (Morne Brits) who will be able to provide a response.

If you would like to make a SAR in relation to your own personal data, you should make this in writing to Director of Operations. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

Your data subject rights.

You have the right to information about what personal data we process, how and on what basis as set out in this policy.

You have the right to access your own personal data by way of a subject access request (see above).

You can correct any inaccuracies in your personal data. To do so you should contact the Director of Operations. You have the right to request that we erase your personal data where we were not entitled under the law to process it, or it is no longer necessary to process it for the purpose it was collected. To do so you should contact the Director of Operations.

While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact the Director of Operations.

You have the right to object to data processing where we are relying on a legitimate interest to do so, and you think that your rights and interests outweigh our own and you wish us to stop.

You have the right to object if we process your personal data for the purposes of direct marketing.

You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

With some exceptions, you have the right not to be subjected to automated decision-making.

You have the right to be notified of a data security breach concerning your personal data.

In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw consent, you should contact the Director of Operations.

You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk) – to access further information on your rights and our obligations.

Email Acceptable Usage Policy.

The following is guidance on the acceptable use of email according to Industry best practices at the time of publication:

- E-mails should be viewed as any other form of business communication. They should be polite and factual. Be aware that e-mails can be forwarded to other parties outside of your control.
- Take care in mentioning the names (or other identifying factors) of other employees and the employees of companies with whom we do business. They have their own rights of privacy – and if you are unsure, contact your manager or the Director of Operations (Morne Brits).
- Never attach any document to an e-mail (whether text, financial data, or anything else) without it being first encrypted using the encryption software provided for you to use.
- E-mails must not contain any swear words or phrases which could be considered offensive. Your line manager can provide further guidance as required.
- All e-mails should comply with our equal opportunities policy/anti-harassment policy. Remarks or jokes sent by e-mail can amount to harassment and, as with all harassment complaints, the intention of the party sending the e-mail is not relevant. E-mails could well form the foundation of a discrimination claim when they contain remarks or jokes related to race, sex, sexual orientation, disability, age, or religion/belief which one of the recipients finds offensive.
- Do not tamper with anyone else's e-mail account. Specifically, do not send an e-mail which appears to originate from someone else but was typed by you.
- Do not forward someone else's e-mail for non-business-related reasons.
- Keep e-mails brief and business like.
- Avoid copying your colleagues into e-mails unnecessarily.

Internet Acceptable Usage Policy.

The following is guidance on the acceptable use of Internet according to Industry best practices.

at the time of publication:

- Internet searches and activity should be strictly business related.
- Searches must not contain any swear words or phrases which could be considered offensive.
- All internet activity should comply with The Proximity Group Ltd.'s equal opportunities and the policies set out by Proximity Healthcare. Remarks or jokes sent by internet channels can amount to harassment and, as with all harassment complaints, the intention of the party sending the e-mail is not relevant. Internet based comments could well form the foundation of a discrimination claim when they contain remarks or jokes related to race, sex, sexual orientation, disability, age, or religion/belief which one of the recipients finds offensive.
- Do not tamper with or use anyone else's network account for internet usage.
- For more information on Social Media, please see the Social Media Acceptable Use Policy. Subject to the balance of this policy, employees may use the Internet access provided by The Proximity Group Ltd for:
 - Work-related purposes.
 - Sending and receiving personal email messages, provided that if email messages are sent with The Proximity Group Ltd email address in the From: or Reply-To: header, a disclaimer shall accompany the email to the effect that the views of the sender may not represent those of The Proximity Group Ltd.
 - Reading and posting personal Usenet messages on the same condition specified above.
 - Using instant messaging software for personal purposes.
 - Accessing the World Wide Web for personal purposes.
 - Utilising any other Internet service or protocol for personal purposes after obtaining permission to do so from The Proximity Group Ltd. Provided in each case that the personal use is moderate in time, does not incur significant cost for The Proximity Group Ltd and does not interfere with the employment duties of the employee or his or her colleagues. Except during an employee's duties or with the express permission of The Proximity Group Ltd the Internet access provided by The Proximity Group Ltd may not be used for:
 - personal commercial purposes.
 - sending unsolicited bulk email.
 - disseminating confidential information of The Proximity Group Ltd.
 - disseminating the names, addresses and other personal data of The Proximity Group Ltd employees or the employees of other companies with which The Proximity Group Ltd does business or has contact.
 - any illegal purpose.
 - knowingly causing interference with or disruption to any network, information service, equipment, or any user thereof.
 - disseminating personal contact information of officers or employees of The Proximity Group Ltd without their consent; and
 - causing any other person to view content which could render The Proximity Group Ltd liable pursuant to equal opportunity, equality, or sex discrimination legislation at the suit of that person or downloading or requesting software or media files or data streams that the employee has reason to believe will use a greater amount of network bandwidth than is appropriate.

Responsibility for use of the Internet that does not comply with this policy lies with the employee so using it, and such employee must indemnify The Proximity Group Ltd for any direct loss and reasonably foreseeable losses suffered by The Proximity Group Ltd by reason of the breach of policy. This may have a significant legal and financial impact on the employee and their family.

The Proximity Group Ltd will review any alleged breach of this Acceptable Use Policy on an individual basis. If the alleged breach is of a very serious nature which breaches the employee's duty of fidelity to The Proximity Group Ltd (for example, emailing confidential information of The Proximity Group Ltd to a competitor), the employee shall be given an opportunity to be heard in relation to the alleged breach and if it is admitted or clearly established to the satisfaction of The Proximity Group Ltd the breach may be treated as grounds for dismissal.

Social Media Acceptable Use Policy.

Any communications that employees make in a professional capacity through social media must not:

- make defamatory comments about individuals or other organisations or groups.
- give away confidential information about an individual (such as a colleague or partner contact) or organisation (such as a partner institution).
- breach confidentiality (for example, by revealing confidential intellectual property or information owned by The Proximity Group Ltd).
- discuss The Proximity Group Ltd.'s internal workings (such as agreements that it is reaching with partner institutions/customers or its future business plans that have not been communicated to the public).
- do anything that could be considered discriminatory against, or bullying or harassment of, any individual (for example by making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age).
- use social media to bully another individual (such as an employee of The Proximity Group Ltd).
- post images or links to content that could be considered inappropriate, discriminatory, or offensive.
- bring The Proximity Group Ltd into disrepute (for example by criticising or arguing with customers, colleagues, partners, or competitors).
- breach copyright (for example by using someone else's images or written content without permission).
- breach Data Protection and Privacy Law (for example by naming other people and/or giving out details about them); and
- fail to give acknowledgement where permission has been given to reproduce something.

Any communications that employees make in a personal capacity through social media must not:

- make defamatory comments about individuals or other organisations or groups.
- breach confidentiality (for example by revealing confidential intellectual property or information owned by The Proximity Group Ltd).
- give away confidential information about an individual (such as a colleague or partner contact) or organisation (such as a partner institution).
- discuss The Proximity Group Ltd.'s internal workings (such as agreements that it is reaching with partner institutions/customers or its future business plans that have not been communicated to the public).
- do anything that could be considered discriminatory against, or bullying or harassment of, any individual (for example by making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age).
- use social media to bully another individual (such as an employee of The Proximity Group Ltd).
- Post images or links to content that could be considered inappropriate, discriminatory, or offensive.
- bring The Proximity Group Ltd into disrepute (for example by criticising or arguing with customers, colleagues, partners, or competitors).
- breach copyright (for example by using someone else's images or written content without permission).
- breach Data Protection and Privacy Law (for example by naming other people and/or giving out details about them).
- fail to give acknowledgement where permission has been given to reproduce something.

Corporate Infrastructure Policy.

Corporate Infrastructure refers to all hardware, software, networks, and information technology procured and controlled by The Proximity Group Ltd.

You are responsible for the security of data, accounts, and systems under your control:

GDPR and Data Privacy Policy-2024

- You must maintain system-level and user-level passwords in accordance with the following Password Policy:
 - o Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends.
 - o All PCs, PDAs, Smartphones, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
 - o Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.
- You must ensure through legal or technical means that The Proximity Group Ltd proprietary information; and the personal data that The Proximity Group Ltd is responsible for always remains within the control of The Proximity Group Ltd.
- You are responsible for ensuring the protection of assigned The Proximity Group Ltd assets:
 - o Laptops left at The Proximity Group Ltd overnight must be properly secured or placed in a locked drawer or cabinet.
 - o Promptly report any theft to one of The Proximity Group Ltd.'s Directors or your immediate line manager.
- Devices that connect to The Proximity Group Ltd network must comply with the following Minimum

Access Policy:

- o The Proximity Group Ltd business that results in the storage of proprietary information on personal or non-The Proximity Group Ltd controlled environments, including devices maintained by a third party with whom The Proximity Group Ltd does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by, The Proximity Group Ltd or its customer and partners, for company business.
- o Employees personal devices must only be used on wireless networks specifically provided by The Proximity Group Ltd for personal usage. They must not be connected to any of The Proximity Group Ltd.'s business networks or used for any The Proximity Group Ltd business activity without the prior written consent of at least one of The Proximity Group Ltd.'s Directors.
 - Do not interfere with corporate device management or security system software, including, but not limited to antivirus, device management or security software products and tools maintained by The Proximity Group Ltd. You are responsible for the security and appropriate use of The Proximity Group Ltd network resources under your control. Using The Proximity Group Ltd resources for the following is strictly prohibited:
 - Causing a security breach to either The Proximity Group Ltd or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized circumventing user authentication on any device; or sniffing network traffic.
 - Causing a disruption of service to either The Proximity Group Ltd or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.
 - Taking or assisting the taking of company records that contains the names, addresses and other details of persons (even if they are employees of The Proximity Group Ltd or another company) outside The Proximity Group Ltd network resources.
 - Introducing honeypots, honeynets, or similar technology on the The Proximity Group Ltd network.
 - Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software. See the The Proximity Group Ltd for additional information on copyright restrictions.
 - Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws.

- Use of the Internet or The Proximity Group Ltd network that violates the any of The Proximity Group Ltd policies, or local laws.
- Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers.
- Port scanning or security scanning on a production network unless authorized in advance by Information Security.

Business Application Policy.

The following Business Applications are approved for use on Corporate Infrastructure and BYOD devices used for business purposes:

1. Outlook
2. Excel
3. Word
4. MS Project
5. Skype
6. Zoom
7. MS Teams
8. WhatsApp
9. TempAlly
10. HubSpot

Business Applications not on this list must not be used for business purposes under any circumstances. Transfer of data from approved Business Applications to non-approved Business Applications is strictly prohibited and will be considered misconduct.

The following is a non-exhaustive list of non-approved Business Applications:

1. Facebook
2. Twitter
3. Cloud Services
4. Bring Your Own Device (BYOD) SMS

Infrastructure Monitoring Policy

The Proximity Group Ltd recognise the employee's right to privacy and our responsibilities under law. In particular:

- We recognise that employees have a right to privacy in respect of their personal communications.
- We reserve the right to monitor employ warning-mail and the Internet to ensure compliance with The Proximity Group Ltd.'s Email Usage, Internet Usage and Social Media Acceptable Use policies and to investigate any specific breaches of the policy where there is sufficient reason to do so Prior to monitoring, The Proximity Group Ltd will carry out an impact assessment to assess the necessary extent of any monitoring, the nature of any adverse effect upon the employee and the safeguards required to an employee e.g. prior warning.

Monitoring will be conducted with the authorisation of a line manager on prior notice to the employee concerned.

Monitoring may include any of the following:

- Reviewing Internet sites accessed.
- Reviewing time spent on e-mail and internet.
- Reviewing e-mails sent and received.
- Reviewing files attached to e-mails.
- Reviewing Uploads.

- Reviewing Downloads.
- Reviewing non-business behaviours.

This list is not exhaustive, and we reserve the right to use other techniques. Covert monitoring (i.e. where no warning is given) shall only be used where it is:

- Required by regulatory/legal obligations.
- Necessary to prevent or detect crime.
- Required to protect The Proximity Group Ltd.'s IT systems from damage (e.g. viruses).
- Gross misconduct is suspected.

The information will be collated by the individual monitoring and shared with the employee as soon as practical – this may be as part of an investigation conducted under The Proximity Group Ltd.'s disciplinary process.