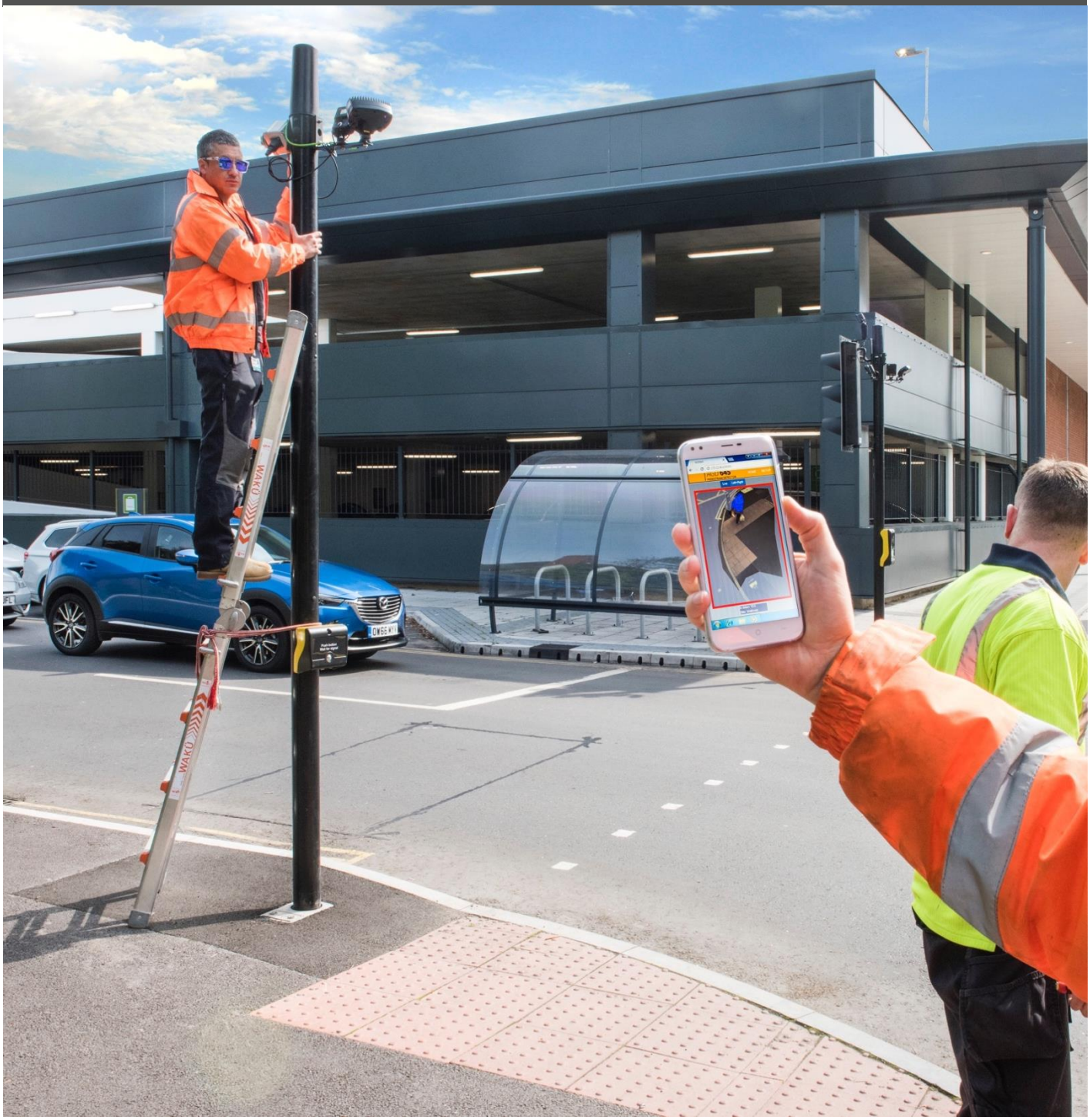
PRODUCT SOLUTIONS FOR
INTELLIGENT TRAFFIC SYSTEMS

BUSINESS POLICIES



A guide to the Business Policies at AGD Systems Ltd and Traffic Group Technology

THE TRAFFIC GROUP

PRODUCT SOLUTIONS FOR
INTELLIGENT TRAFFIC SYSTEMS

BUSINESS POLICIES

MANUAL NO:	MASTER
MANUAL ISSUE:	05
DATE OF ISSUE:	26/8/22

THESE POLICIES ARE APPROVED FOR ISSUE BY:-

Managing Director

COMPANY MISSION:

"To be recognised as the supplier of choice for technologically superior sustainable detection equipment for transport".

Table of Contents

AGD SYSTEMS LTD – ENVIRONMENTAL AND SOCIAL RESPONSIBILITY POLICY

AGD Systems Ltd design, develop and manufacture information and measurement equipment to meet the requirements of global transport management industries and users.

A keyway to achieve this is by operating an Environmental Management System (EMS) in accordance with the requirements of ISO 14001: 2018.

Statement of Intent

The board of directors at AGD Systems Ltd is committed to providing an ethical working environment and to the protection of the environment whilst developing its business towards ecological, social and economic sustainability. To this end we have documented, implemented and maintained an Environmental Management System. The tasks are recognised as shared responsibilities within AGD Systems enabling a continuous improvement of our operations.

Policy Aims

AGD Systems will work for long-term, sustainable development by offering product designs that take the environment into consideration during the entire product life cycle and prevents unnecessary negative effects on the environment. We expect the same commitment from our suppliers and customers so that at every stage, from raw material to end product use, the impact on the environment will be minimized.

We, as a company are committed to:

Compliance with all statutory and regulatory requirements related to our activities, products and services and their environmental aspects and in-line with the context of the organisation and having considered our interested parties.

Establishing design and purchasing standards that will promote the use of environmentally friendly processes and materials, and that will encourage the development of products that can be re-used, recycled or disposed of safely and in an environmentally sound way.

Designing energy efficiency into new products, services and facilities, and manage energy use responsibly in all areas of the business.

Continually improving targets and objectives to prevent and reduce pollution and avoid waste at all times and reduce our impact on the environment.

Working with and encouraging our suppliers and customers to minimise the impact of their activities on the environment and pursue best practice.

Promoting environmental awareness and responsibility and recognising and encouraging the contribution each employee can make towards improving environmental performance.

Aiming to continually improve our quality and environmental management processes by setting and reviewing objectives and targets.

Seeking to reduce the impact of the company's activities on the local environment and be a good neighbour in the community.

This policy is available to the public and has been communicated to all the employees.

Social Respect

As an international company, AGD Systems acknowledges its role within the global, national and local society. Our attitude shall be characterised by respect for the cultures, customs and values of individuals and groups in countries where we operate. AGD is committed to an ethical working environment that respects our employee's human rights and freedom. We have a zero-tolerance approach to modern slavery and human trafficking within our business and with our third parties. When developing our business to earn credibility, we will comply to and when necessary go beyond the requirements of national standards and legislation.

Managing Director

AGD SYSTEMS LTD – QUALITY POLICY STATEMENT

AGD is a privately owned & independent UK company dedicated to the design, development & manufacture of traffic detection & associated products and has a vision to be synonymous with professionalism and innovation within our chosen markets.

A keyway to achieve this is by operating a Quality Management System (QMS) in accordance with the requirements of ISO 9001: 2018 and the National Highways Sector 8 Scheme. Scope: The design, development and manufacture of information and measurement equipment, including the provision of associated and related services, to meet the requirements of the transport management industries and users. Incorporating the provision, installation and maintenance, of highway electronic equipment in compliance with the National Highway Sector Scheme 8.

The Directors are committed to:

Satisfying applicable requirements by ensuring that both customer and relevant statutory and regulatory requirements are determined, understood and consistently met in-line with the context of the organisation and having considered our Interested parties.

Continual improvement of the QMS by ensuring the risks and opportunities that can affect conformity of products and services and the ability to enhance customer satisfaction are determined and addressed and the focus on enhancing customer satisfaction is maintained.

The Directors shall:

Take accountability for the effectiveness of the QMS.

Ensure the quality policy and quality objectives are established for the QMS and are compatible with the context and strategic direction of the Company. Quality objectives have been set and are maintained as part of the QMS internal auditing, monitoring and management review processes, in order to enhance customer satisfaction.

Promote the use of a process approach and risk-based thinking.
Ensure that the resources needed for the QMS are available; including training, support and encouragement.
Communicate the importance of effective quality management and of conforming to the QMS requirements.
Engage, direct and support persons to contribute to the effectiveness of the QMS.
Promote improvement and ensure that the QMS achieves its intended results.
Support other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.
Establish partnerships with suppliers and interested parties to provide an improved service.
This policy will be communicated to all employees, is available to relevant interested parties, will be reviewed annually by top management and where deemed necessary will be amended and re-issued.

Core Business Objectives: The objectives are reviewed through KPI performance study during the BIC meetings.

- Increasing product reliability and customer perception
- Improving supplier performance
- Reducing material costs
- Increasing patents
- Increasing turnover/market share

Transitional: Specific targets are assigned through results of internal audits, business improvement committee meetings, legislation or customer/interested party requirements. These transitional targets are regularly reviewed.

Managing Director

AGD SYSTEMS LTD – OCCUPATIONAL HEALTH & SAFETY POLICY STATEMENT

AGD is a privately owned & independent UK company dedicated to the design, development & manufacture of traffic detection & associated products and has a vision to be synonymous with professionalism and innovation within our chosen markets.

The AGD Systems Health and Safety Policy applies to all operations including transient work sites.

The Managing Director recognises and accepts responsibility to provide a safe and healthy working environment and to prevent injury and ill health for all employees, sub-contractors and visitors who attend AGD premises and transient work sites and others (e.g. public, client workers) who may be affected by the conduct of our operations. By signing this Occupational Health and Safety Policy, the Managing Director gives approval to the Occupational Health and Safety Management System described in the Integrated Management System Manual and in supporting Company Processes.

AGD Limited recognises the social and economic importance of protecting the health and safety of those affected by its operations and is committed to leading by example in promoting health and safety in all its operations. Health and safety should never be compromised for any other objective.

This Occupational Health and Safety Policy is evaluated as part of the overall review of the Occupational Health and Safety Management System to ensure its stated objectives are met.

HEALTH AND SAFETY COMMITMENT, OBJECTIVES AND PRINCIPLES

Our commitment, objectives and principles of the Occupational Health and Safety (OH&S) Policy are:

- To provide and maintain an Occupational Health and Safety Management System which satisfies the requirements of ISO 45001:2018, all applicable legal and other requirements, industry best practice and any other Client specific requirements.

- To provide safe and healthy working conditions for the prevention of work-related injury, ill health or mental health and is appropriate to the purpose, size and context of AGD and to the specific nature of our OH&S risks and opportunities.

- To maintain workplaces to ensure that they are safe and without health risks, including means of access and egress, with adequate facilities and arrangements for employees' welfare.

- To provide and maintain working environments and safe systems of work for employees and to eliminate hazards and reduce OH&S risks.

- To provide and maintain plant and equipment and operational controls that prevent injury and ill health and to ensure safety and absence of health risks in connection with the use, handling and storage of articles and substances.

- To consult and participate with employees and where they exist workers representatives on issues relating to occupational health and safety.

- To promote and encourage a positive health and safety culture throughout the organisation through the provision of information, training, instruction and supervision.

- To provide sufficient information, instruction, training and supervision to enable employees to avoid hazards and to contribute positively to the health and safety of themselves and others whilst at work.

- To establish effective arrangements to draw the Occupational Health and Safety Management System to the attention of employees so that they are aware of their obligations and carry out communication so it is understood and implemented by all employees.

- To ensure all employees are aware of their individual occupational Health and Safety obligations under the Health and Safety at Work etc Act. Management shall seek the support and co-operation of employees with respect to occupational health and safety.

- To operate a 'balanced blame' culture whereby employees are openly encouraged to report hazards, including near misses, without fear of reprisal to ensure the root causes of accidents are identified thus enabling measures to be put in place to eliminate recurrence.

- To ensure sufficient financial and physical resources are available to meet the objectives of the Occupational Health and Safety Management System, as well as all applicable statutory and regulatory requirements.

- To provide a framework where occupational health and safety objectives are set, monitored and reviewed at regular intervals.

- To maintain continual improvement of the occupational health and safety management system and performance by regularly monitoring and reviewing the occupational Health and Safety Management System to ensure its effectiveness.

- To update operations in response to advances in technology, changes to industry best practice and new understanding in health and safety.

- To ensure that risk assessments are being carried out on an on-going basis, with employees participating in the risk assessment process. Assessments will cover AGD Systems undertakings and will assist in the identification of hazards and the setting of prioritised objectives for elimination and reduction of risk.

- To arrange for the effective planning, organisation, control, monitoring and review of preventative and protective measures.

- To maintain records as objective evidence to show compliance with the Occupational Health and Safety Management System.

RESPONSIBILITY: The Managing Director has the overall responsibility for the Occupational Health and Safety Policy and Occupational Health and Safety Management System including formulation, development, implementation and encouraging commitment by personnel at all levels of the Company. The Management Representatives nominated in the Integrated Business Manual are responsible for the co-ordination, implementation and monitoring of the policy throughout the organisation. All employees, contractors and visitors are responsible for policy implementation by cooperating, participating and contributing to its success through their actions and suggestions.

COMMUNICATION: This Occupational Health and Safety Policy is communicated to all employees, contractors and visitors. A copy is displayed on employee notice boards and published on the internal company shared drive. All employees are encouraged to read it and communicate any queries to a Director.

Copies are made available to interested parties on request and a copy is published on the company website.

Pete Hutchinson

Managing Director

AGD SYSTEMS LTD – SUPPLY ASSURANCE & ETHICS POLICY

Statement of Intent

AGD's vision is to set the highest standards of partnership throughout the supply chain to create value and sustainable competitive advantage. This is achieved by developing a working relationship based on openness, honesty, integrity and trust.

In an increasingly competitive environment, the financial risk and increase in investment required to develop new products is substantial. The issue of supply chain relationships within and between companies has long been recognised as a key factor influencing our industry and its ability to compete and increase share in world markets.

Customers want to work with performance driven suppliers in the supply chain. We will strive to outperform our competitors supply chain to win end market share and grow business for all participants.

Policy Aims

The aim of this policy is to promote team working within the AGD supply chain by focusing on six key elements;

Communication - Creating an environment that fosters co-operation, openness, and sharing of information will develop trust which enables joint performance improvement.

Through Life Capability Management - AGD will deliver integrated supply solutions utilising the capabilities and knowledge at all levels of the supply chain, to fulfil customer requirements in the most cost-effective way throughout the life of the project, product or service.

Continuous Improvement - Drive a Lean management culture within AGD and between elements of the supply chain, to remove waste and aspire to six sigma levels of quality. Be prepared to share knowledge and experience to enable AGD and its supply chain to be a leader in competitive value chains.

Supplier Qualification and assessment - Supplier qualification and assessment will only be carried out when it is necessary to satisfy AGD of the supplier's capability.

Commercial Agreements - Honest and open communication is vital to achieving successful commercial relationships. The aim of all commercial agreements must be to ensure the deliverables meet customer expectations whilst, at the same time, reducing project costs and lead times so improving profitability, service and product quality up and down the supply chain.

Ethics - All business will be conducted in a principled manner with the highest degree of personal and business integrity.
We have a zero-tolerance approach to modern slavery. We are committed to acting ethically and with integrity in all our business dealings and relationships and implementing and enforcing effective systems and controls to ensure modern slavery is not taking place anywhere in our own business or in any of our supply chains.

Environment - All business will be conducted in a principled manner with the highest degree of personal and business integrity. Environmental awareness and improvements will be achieved by encouraging our suppliers to set environmental targets and achieve ISO 14001 accreditation.

Managing Director

AGD SYSTEMS LTD - ANTI-BRIBERY POLICY

AGD Systems Limited (AGD) strives to undertake our business fairly with honesty and transparency. This must be reflected in every aspect of our business affairs.

The action and conduct of AGD Directors and employees (collectively AGD personnel) as well as others acting on AGD's behalf are essential to maintaining these standards. To that end, all AGD personnel, including agents, consultants and contractors as well as suppliers involved in AGD international business must read, become familiar and comply with this Anti-Bribery Policy.

Compliance with Anti-Bribery Laws

It is AGD's Policy to comply with all laws, rules, and regulations governing anti-bribery and corruption law, in all the countries where we operate. AGD has a zero-tolerance approach to acts of Bribery and corruption, by employees or anyone acting on our behalf. Any breach of this policy will be regarded as a serious matter by the Company of which is likely to result in disciplinary action.

Under UK law (UK Bribery Act 2010), bribery and corruption is punishable for individuals by up to ten years imprisonment. If the company is found to have taken part in the corruption or lacks adequate procedures to prevent Bribery, it could face an unlimited fine and, be excluded from tendering for Government contracts and face untold damage to its reputation.

The payment or offer to pay bribes, or provisions of, or offer to provide gifts or anything of value for improper purposes, to obtain or retain business or any other benefit, (whether for AGD or any other party) is prohibited. Such payments or gifts are also forbidden under the terms of this policy and may result in immediate dismissal for those involved in their payment or receipt.

AGD is required to keep financial records and to have appropriate internal controls in place which will evidence the business reason for making payments to third parties.

Application of the Policy

This policy applies to individual employees, agents, sponsors, intermediaries, consultants or any other people or bodies associated with AGD or any of its subsidiaries and employees. Bribery is committed when an inducement or reward is provided, in order to gain any commercial, contractual, regulatory or personal advantage for AGD or another party.

No bribes of any sort may be paid or accepted from customers, suppliers, politicians, government advisors or representative's private person or Company. It is not permitted to establish accounts or internal budgets for the purpose of making facilitation bribes or influencing transactions (slush funds).

AGD recognise that to refuse a gift in certain circumstances and/or countries would cause offence to our trading partners. The test to be applied in all circumstances is whether the gift or entertainment is reasonable and justifiable. What is the intention of the gift? Is the gift being offered for something in return (quid pro quo). This policy does not prohibit the following practices providing they are customary in a particular market or are appropriate and properly recorded. *Refer to Employee Handbook section 20.13 Gifts to Staff.*

Employee Responsibility

The presentation, detection and reporting of bribery is the responsibility of all employees throughout the Group.

Suitable channels of communication by which employees or others can report confidentially any suspicion of bribery, which will be maintained through AGD's Whistle Blowing Policy see information below.

Reporting incidents of Bribery and Corruption

If you become aware that an activity or conduct which has taken place which you suspect is a bribe (or corrupt). You have a duty to report this. Any such incidents should be reported to your Supervisor/ Line Manager. *Refer to Employee Handbook section 21 Public Interest Disclosure (Whistle Blowing) Policy.*

Managing Director

1. Policy statement

This policy is intended to help staff make appropriate decisions about the use of social media such as blogs, wikis, social networking websites, podcasts, forums, message boards, or comments on web-articles, such as Twitter, Facebook and LinkedIn.

This policy is intended to help staff make appropriate decisions about the use of social media such as blogs, wikis, social networking websites, podcasts, forums, message boards, or comments on web-articles, such as Twitter, Facebook and LinkedIn.

This policy outlines the standards we require staff to observe when using social media, the circumstances in which we will monitor your use of social media and the action we will take in respect of breaches of this policy.

This policy supplements our Internet and E-mail Policy and does not form part of any contract of employment and may be amended at any time.

Who is covered by the policy

This policy covers all individuals working at all levels, including line managers, directors, employees, consultants, contractors, trainees, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as **staff** in this policy).

The scope of the policy

All staff are expected to comply with this policy at all times to protect the privacy, confidentiality, and interests of our company and our services, employees, customers and competitors.

Breaches of this policy will be dealt with through the company's Disciplinary Procedures for staff. These will be implemented at a level appropriate to the seriousness of the alleged misconduct.

Responsibility for implementation of the policy

The Managing Director has overall responsibility for the effective operation of this policy.

The Managing Director is responsible for monitoring and reviewing the operation of this policy and making recommendations for changes to minimise risks to our operations.

All staff are responsible for their own compliance with this policy and for ensuring that it is consistently applied. All staff should ensure that they take the time to read and understand it. Any breach of this policy should be reported to the Managing Director.

Questions regarding the content or application of this policy should be directed to the Managing Director.

Using social media sites in our name

Only the IT Manager / AGD Website Administrators or the trained appointed person are permitted to post material on a social media website in our name and on our behalf. Any breach of this restriction will amount to gross misconduct.

Using work-related social media

We recognise the importance of the internet in shaping public thinking about our company and our services, employees and customers. We also recognise the importance of our staff joining in and helping shape industry conversation and direction through interaction in social media.

Before using work-related social media, you must:

have read and understood this policy and our internet and e-mail policies; and
have sought and gained prior written approval to do so.

Personal use of social media sites

We permit the incidental use of social media websites for personal use subject to certain conditions set out below. However, this is a privilege and not a right. It must neither be abused nor overused, and we reserve the right to withdraw our permission at any time at our entire discretion.

The following conditions must be met for personal use to continue:

(a) use must be minimal and take place substantially out of normal working hours (during lunch or break times);

(b) use must not breach any of the rules set out below.

(c) use must not interfere with business or office commitments;

(d) use must comply with our policies including Equal Opportunities Policy, Harassment Policy, Data Protection Policy and Disciplinary Procedure.

Rules for use of social media

Whenever you are permitted to use social media in accordance with this policy, you must adhere to the following general rules:

- Always write in the first person, identify who you are and what your role is, and use the following disclaimer "The views expressed are my own and don't reflect the views of my employer".
- Do not upload, post, forward or post a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content.
- Any member of staff who feels that they have been harassed or bullied or are offended by material posted or uploaded by a colleague onto a social media website should inform their line manager.
- Never disclose commercially sensitive, anti-competitive, private or confidential information. If you are unsure whether the information you wish to share falls within one of these categories, you should discuss this with your line manager.
- Do not upload, post or forward any content belonging to a third party unless you have that third party's consent.
- It is acceptable to quote a small excerpt from an article, particularly for the purposes of commenting on it or criticising it. However, if you think an excerpt is too big, it probably is. Quote accurately, include references and when in doubt, link, don't copy.
- Before you include a link to a third-party website, check that any terms and conditions of that website permit you to link to it. All links must be done so that it is clear to the user that they have moved to the third party's website.
- When making use of any social media platform, you must read and comply with its terms of use.
- Do not post, upload, forward or post a link to chain mail, junk mail, cartoons, jokes or gossip.
- Be honest and open but be mindful of the impact your contribution might make to people's perceptions of us as a company. If you make a mistake in a contribution, be prompt in admitting and correcting it.
- You are personally responsible for content you publish into social media tools – be aware that what you publish will be public for many years.

  Do not escalate heated discussions, try to be conciliatory, respectful and quote facts to lower the temperature and correct misrepresentations. Never contribute to a discussion if you are angry or upset, return to it later when you can contribute in a calm and rational manner.
- If you feel even slightly uneasy about something you are about to publish, then you should not do it. If in doubt, always discuss it with your line manager first.
- Don't discuss colleagues, competitors, customers or suppliers without their prior approval.

- Always consider others' privacy and avoid discussing topics that may be inflammatory e.g. politics and religion.
- Avoid publishing your contact details where they can be accessed and used widely by people you did not intend to see them, and never publish anyone else's contact details.
- Before your first contribution on any social media site, observe the activity on the site for a while before launching in yourself to get a feel for the style of contributions, the nature of the content and any 'unwritten' rules that other contributors might follow.
- Activity on social media websites during office hours should complement and/or support your role and should be used in moderation.
- If you notice any content posted on social media about the company (whether complementary or critical) please report it to your line manager.

Monitoring use of social media websites

Staff should be aware that any use of social media websites (whether or not accessed for work purposes) may be monitored and, where breaches of this policy are found, action may be taken through the company's Disciplinary Procedures.

We reserve the right to restrict or prevent access to certain social media websites if we consider personal use to be excessive. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against you and us. It may also cause embarrassment to us and to our customers.

In particular uploading, posting forwarding or posting a link to any of the following types of material on a social media website, whether in a professional or personal capacity, will amount to gross misconduct (this list is not exhaustive):

(a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

(b) a false and defamatory statement about any person or organisation;

(c) material which is offensive, obscene, criminal discriminatory, derogatory or may cause embarrassment to us, our clients or our staff;

(d) confidential information about us or any of our staff or clients (which you do not have express authority to disseminate);

(e) any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us); or

(f) material in breach of copyright or other intellectual property rights, or which invades the privacy of any person.

Any such action will be addressed through the company's Disciplinary Procedures and is likely to result in summary dismissal.

Where evidence of misuse is found we may undertake a more detailed investigation in accordance with the company's Disciplinary Procedures involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the investigation. If necessary, such information may be handed to the police in connection with a criminal investigation.

If you notice any use of social media by other members of staff in breach of this policy, please report it to your line manager.

Monitoring and review of this policy

The Managing Director shall be responsible for reviewing this policy annually to ensure that it meets legal requirements and reflects best practice.

The use of social media outside of work:

As social media is largely used in a personal context, it is important for employees to remember that the Internet is a public space and posts on such sites are in the 'public domain'. Even with stringent security settings, content is at risk from security breaches and / or being published elsewhere. As such, content posted online by an employee could have adverse effects on AGD and its associated parties.

If social networking sites are used outside of work, the employee must not:

- Discuss work related issues
- Disclose key business knowledge that could be used by competitors
- Cite or reference any colleagues, clients, customers, partners or suppliers without obtaining their express permission to do so, even if their specific names are not mentioned
- Post content or behave in such a way that could bring the company name into disrepute
- Insult or disparage AGD, its products or services
- Publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the AGD into disrepute.
- Breach AGD's misconduct, equal opportunities or bullying and harassment policies

The employee is responsible for reading, knowing and complying with the Terms of Service of the sites they use.

Breach of this policy will be taken seriously and can result in disciplinary action, up to and including dismissal, depending on the nature and impact of the breach.

Confidentiality

You must not during the period of your employment divulge to any outside body any trade secrets, confidential information, research product knowledge, client details, pricing lists and details of business connections including such of the foregoing that you have introduced into the Company during your employment.

You must not after termination of your employment divulge or use for your own purposes any trade secrets , confidential information, research product knowledge, business connections, client/customer details, pricing arrangement of the Company including such of the aforementioned that you during the course of your employment introduced to the Company.

You shall not remove from the place of employment any documentation of any description including computer/disk based information nor take copies of such documentation for your personal use or the use of a competitor or third party either during your employment or on termination of your employment.

Any information provided by the Company to you will be regarded as confidential unless it is of a type that would be:-

freely available to the general public;

freely available to members of the Company's trade or profession.

Managing Director

AGD is committed to the principle of equal opportunities in employment and declares its opposition to any form of less favourable treatment, whether through direct or indirect discrimination accorded to employees or job applicants, on the grounds of age, disability, gender reassignment, marriage or civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation (defined as Protected Characteristics)

AGD recognises its obligations under the Equality Act 2010 and the spirit and intent of any related Codes of Practice:

- for the elimination of discrimination on grounds of sex or marital status and the promotion of equality of opportunity in employment;
- for the elimination of discrimination on grounds of race and the promotion of equality of opportunity in employment;
- for the elimination of discrimination on the grounds of disability and the promotion of equality of opportunity in employment;
- for the elimination of discrimination on the grounds of religion or belief and the promotion of equality of opportunity in employment;
- for the elimination of discrimination on the grounds of sexual orientation and the promotion of equality of opportunity in employment.
- for the elimination of discrimination on the grounds of age and the promotion of equality of opportunity in employment;
- for the elimination of discrimination because they associate with another person who possesses a Protected Characteristic or because others perceive that they have a particular Protected Characteristic, even if they do not.

Employment Practices

AGD states its wholehearted support for the principles and practices of equal opportunity and recognises that it is the duty of all employees to accept their personal responsibility for fostering a fully integrated community at work by adhering to the principles of equal opportunity and maintaining a harmonious working environment. We believe as part of these principles that employees should receive equal pay for work of equal value.

AGD actively promotes equal opportunities throughout the organisation through the application of employment policies which will ensure that individuals receive treatment that is fair and equitable and consistent with their relevant aptitudes, potential, skills, experiences and abilities. All Managers and Supervisors will seek to ensure that all employees comply with these principles.

AGD will ensure that individuals are recruited and selected, paid, promoted and trained on objective criteria having regard to the relevant aptitudes, potential, skills, experiences and abilities. In particular, no applicant will be placed at a disadvantage by any practices which, although they are applied to all, have the effect of disadvantaging people on the grounds of any Protected Characteristic which is not necessary to the performance of the job or which constitute indirect discrimination. Reasonable adjustments will be taken where a person is put in a detrimental position and such reasonable adjustments remove the detriment.

AGD recognises that in order to achieve equal pay for employees carrying out equal work we should operate a pay system which is transparent, based on objective criteria and free from unfair bias on any grounds. In order to do this, AGD are committed to ensuring that it carries out regular monitoring of the impact of pay policies and practices and takes appropriate remedial action to resolve issues identified;

Provides guidance for managers involved in decisions about recruitment, pay, benefits and promotions;

Responds promptly to any complaints in relation to equal pay.

AGD recognises the problems that harassment may cause at work and is committed to ensure that such unacceptable behaviour does not take place. Harassment is unwanted conduct that violates a person's dignity or creates an intimidating, hostile, degrading, humiliating or offensive environment for them having regard to all the circumstances including the perception of the victim. All forms of harassment are abhorrent and will not be tolerated by the Company. Harassment in any form is regarded as unlawful discrimination and additionally may also be subject to criminal proceedings. All such cases will be dealt with under the Disciplinary and Dismissal Procedure.

AGD recognises that the detriment a disabled person endures as a consequence of their disability can, in many instances, be removed by the adoption of reasonable adjustments. The Company is committed to ensure that such adjustments will be affected where reasonably practicable and where the detriment is substantial.

Monitoring and Review Arrangements

AGD recognises that the regular monitoring of employees and job applicants is essential to the thorough review of the effectiveness of this Policy and to this end the Company will initiate equal opportunity monitoring.

The successful implementation of this Policy depends upon the regular examination and progress towards equal opportunity.

AGD will review the physical features and arrangements affecting any newly disabled employee and will take such steps as is reasonable to prevent substantial disadvantage.

Grievance, Disciplinary and Dismissal Procedures

AGD will ensure that any individual or group of employees who believe that they have experienced direct, or indirect discrimination are properly represented in any grievance proceedings. Any employee who feels that he or she has been treated unfairly in connection with their employment should raise their grievance through the Grievance Procedure when every effort will be made to secure a satisfactory resolution. In addition, AGD will ensure that any employee making a complaint of unfair discrimination (or any employee assisting or representing the complainant) will be protected from any victimisation. Where the complaint relates to alleged harassment, the procedure outlined at Section 9, should be followed.

AGD will treat unfair discriminatory conduct or harassment by any member of staff as a serious disciplinary offence.

Whilst the objectives of this policy are clearly stated, and are to be followed, for reasons of equity and justice, it must be advised that any employee who raises a complaint, which upon investigation is proven to be deliberately false, then that employee may themselves become the subject of disciplinary proceedings.

Training and Advertising

AGD will train, develop and promote on the basis of merit and ability only. Where appropriate AGD will seek to encourage employees and job applicants of underrepresented groups by using the positive action measures available to the Company through the relevant legislation.

When vacancies are advertised both internally and externally, AGD will continue to ensure that such advertising, both in placement and content, is compatible with the terms of this Policy. To this end, opportunities will be taken through language, images or declarations, as appropriate, to show that the Company is an equal opportunity employer. In practical terms this means that the wording of advertisements is carefully scrutinised to ensure that any hidden discrimination is avoided, or discriminatory loaded wording is avoided. Every effort will be made to ensure that the advertisements are placed in newspapers and publications so that as wide a readership as possible has access to the vacancies. This may include the placing of advertisements in ethnic publications and women's magazines.

Communication

The principles in this Policy will be brought to the attention of all staff by means of publication in the Employee Handbook.

All employees are encouraged to bring to the attention of their immediate Superior any act of discrimination they observe.

Employees who are newly disabled are encouraged to bring this to the attention of their immediate Superior to enable a review of

their treatment to be made. This review will include an assessment of physical features and arrangements to ensure that these do not place the disabled person at a substantial disadvantage. Where they do, then adjustments will be affected where reasonable to

do so.

Bullying and Harassment

Preamble

This policy is concerned with the prevention of harassment and bullying in the workplace and aims to provide a remedy for unreasonable or unjustifiable behaviour.

Harassment in the employment situation is unlawful under discrimination legislation and as a consequence is unlawful behaviour. It is also improper and inappropriate behaviour which lowers morale and interferes with the effectiveness of people at work.

It is the policy of this organisation to make every effort to provide a working environment free from all forms of harassment, bullying and intimidation.

All employees are expected to comply with the policy and to ensure that such conduct does not occur. Appropriate disciplinary action including summary dismissal for serious offences will be taken against any employee who violates this policy.

Definition

Bullying and harassment are often used interchangeably but in general terms, harassment is unwanted conduct that violates a person's dignity or creates an intimidating, hostile, degrading, humiliating or offensive environment for them having regard to all the circumstances including the perception of the victim. The key is that the actions or comments are viewed as demeaning and/or unacceptable to the recipient. This includes behaviour that an employee may find offensive even if it is not directed at them and they do not possess the relevant protected characteristic. Harassment may come from other employees or by people (third parties) who are not employed by AGD, such as customers or clients.

Bullying can be characterised as offensive, intimidating, malicious or insulting behaviour, an abuse or misuse of power through means intended to undermine, humiliate, denigrate or injure the recipient.

Employees should be aware that this policy covers behaviour in the workplace and when engaged in work-related activities such as social activities held off site or out of normal working hours.

Examples

The following are examples of inappropriate behaviour covered by this Policy:-

Physical conduct of a sexual nature: unwanted physical contact including unnecessary touching, patting, pinching or brushing up against another employee's body, assault.

Verbal conduct by nature of a sexual, racial, sexually orientated, or on the grounds of religion or belief: unwelcome sexual advances, propositions or pressure for sexual activity, continued suggestions for social activity outside the workplace after it has been made clear that such suggestions are unwelcome, offensive comments on sexual orientation, spreading malicious rumours, ridicule or demeaning someone e.g. picking on them or setting them up to fail.

Non-verbal conduct of an offensive nature: the display of pornographic or sexually suggestive pictures, objects or written materials, leering, whistling or making sexually suggestive gestures.

Conduct which denigrates or ridicules or is intimidatory or physically abusive to an employee, such as derogatory or degrading abuse or insults, exclusion or victimisation, overbearing supervision or misuse of power or position or offensive comments about dress or appearance or physique, hygiene etc.

Duty of Managers and Supervisors

All Directors, Managers and Supervisors are responsible for eliminating any forms of harassment, bullying or intimidation of which they are aware. Failure to do so will be treated as a failure to fulfil all the responsibilities of their position. Similarly, all Directors, Managers and Supervisors are responsible for eliminating less favourable treatment of disabled persons for a reason or reasons which relate to their disability. Again, failure to do so will be treated as a failure to fulfil all the responsibilities of their position.

No Director, Manager or Supervisor shall threaten or insinuate, either explicitly or implicitly, that an employee's rejection of sexual advances or resistance to any racial abuse or abuse on the grounds of age, sexual orientation, religion or belief, will be used as a basis

for an employment decision affecting that employee. Such conduct shall be treated by AGD as a serious disciplinary offence by that Director, Manager or Supervisor.

Harassment Complaints Procedure

It is clearly inappropriate for the normal grievance procedure to be used for complaints of harassment particularly where the manager is the alleged harasser.

Wherever possible the person who believes that they are the subject of harassment or bullying should ask the person responsible to stop the offending behaviour. Where this does not stop, or some employment consequences result than a complaint should be made.

An employee who believes that they have been the subject of harassment or bullying should report the alleged act to the appropriate Line manager, Director or a nominated officer of the employee's choice.

A timely investigation will be conducted into the complaint in a confidential manner. All parties will be guaranteed a fair and impartial hearing.

In any serious case of alleged harassment either or both of the parties may be suspended on full pay pending the completion of the investigation.

The victim will be interviewed preferably by a person of the same sex/race where appropriate. Confidentiality will be assured. A diary should be kept by the victim of the details of the allegations and dates when they occurred.

If the investigation reveals that the complaint is valid, senior management will give it its prompt attention and disciplinary action will be taken to stop the harassment

immediately and prevent its recurrence. In such circumstances if relocation proves necessary, every effort will be made to relocate the harasser and not the victim.

Employees shall also be protected from intimidation, victimisation or discrimination for filing a complaint or assisting in an investigation. Retaliation against an employee for complaining about harassment is a disciplinary offence and is also actionable through the Employment Tribunals.

Employees should also use this approach if they feel that they have been the subject of harassment from someone who is not an employee of AGD. AGD will not tolerate any harassment from third parties towards its employees and will take appropriate action to prevent it happening again.

Managing Director

It is the policy of AGD Systems Limited to utilise Information Technology (IT) based hardware and software for the efficient running of the business. Where possible the IT infrastructure shall be of a harmonious nature, from reputable sources (including IT consultancy) and maintained in scale to the business operation.

Business data (digital) important for the maintenance of the business operation shall be regularly backed-up and appropriately stored for safe-recovery.

All data processed shall be in accordance with Notification guidelines with appropriate registration unless exemption is appropriate.

IT infrastructure shall be installed, maintained and available whilst compliant with appropriate Health and Safety requirements.

It is the policy that all software utilised within the IT infrastructure is licensed and used in accordance with the conditions of that licence.

Persistent troublesome hardware/software shall be the subject of ongoing review until a successful remedial solution is implemented. All data from indiscriminate sources entering the infrastructure shall be emailed into the system to ensure integrity.

Appropriate email/internet facilities shall be made available to employees for the efficient despatching of tasks.

Statement of Information Security Policy

The Board of Directors observes both legal and moral obligations relating to Personally Identifiable Information (PII). The organisation prides itself on a simple & honest approach with data subjects & strives to keep up-to-date with the latest technologies & legislation.

Notification

Recognised under the Global Data Protection Regulation as a Data Controller, it is policy of the organisation to maintain accurate notification with the Information Commissioner whether exempt or not. It is policy to update the notification as required & Senior Management will meet annually to review.

Collection of Data

It is policy of the organisation to present honest, accurate information to the subject prior to collection, wherever such information can be presented within reasonable effort.

Collection in relation to employment or sales is covered through terms of employment/sales. Collection from the organisation's websites or online-services will typically feature an "opt-in" to a Privacy Policy and Terms of Service. All other methods will feature the information they can within reason, such as "CCTV in Operation" notices.

Data Transfers

It is policy of the organisation to obtain permission from the subject prior to transferring their details to other companies or countries. In most cases this will be to a subsidiary member or representative of the The Traffic Group within the EEA. The recipient will be expected to adhere to AGD Systems Limited's policies, agreed prior to transfer. Should the recipient lie outside of the EEA, it is policy of the organisation to assess & implement additional security requirements as required.

Subject Access to Data

Where data is held as part of an online service, it is the policy of the company to provide the subject access and control to such details as name, address & contact details. Where deemed suitable to the service, it is policy to offer the subject an option to remove their PII footprint from the online service.

It is policy of the company to process written Subject Access Requests in line with the GDPR. Though it is intended the organisation responds with professional efficiency, currently this a maximum turnaround of 1 month with no fee.

Controlling Physical Security

The following policies have been put in place to help prevent unauthorised access to data storage and data access areas:

- In working hours, all buildings feature secure FOB entry system beyond reception area
- Guests & contractors are accompanied at all times, or are bound in advance to our terms
- Employees are made aware of planned guests/contractors visits & are requested to interrogate unaccompanied and unidentified individuals
- Employees operate a clear-desk policy where personal information is concerned
- When not in use, documents featuring PII is secured in filing cabinets or desk drawers
- When not in use, computer workstations are kept protected by password (locked)
- The Server rooms (containing internally hosted data) is a restricted access area with only the IT Department & Senior Management having access
- Buildings are secured out of hours by managed alarm systems

Controls on Internal & 3rd Party Access to Information

The following policies have been put in place to help prevent unauthorised access to data storage and data access areas:

- Managed (Internally or by ISP) firewall controls external access to internal network
- Managed (Internally or by ISP) firewall controls internal access to external networks
- Internally hosted web servers reside in DMZ with severely restricted domain access
- Externally hosted web servers meet relevant company policies as checked by IT Manager
- Online databanks stored in secured server area not available to clients/browsers
- Employees are allocated relevant access to the network using Windows Active Directory
- Company guests/visitors are given network access only for internet connectivity and are not able to access and company servers or data stored within.
- Passwords are sent encrypted where possible
- During phone calls or enquiries relating to personal information, employees authenticate the data subject by verifying 3 pieces of personal info
- Employees not to use personal devices to access network/terminals without permission from IT Manager
- Employees not to use company devices for personal use without prior permission

Detecting breaches of security

In all new systems, policy applies to help autonomously identify and block malicious access where possible. Furthermore, the data subject will be notified where such breach attempts may affect them.

The organisation has policy to record activity logs relating to systems storing personal data. Where automated systems are not available, the relevant employees are made aware of the responsibilities when monitoring logs & the period in which to monitor.

During design stages, relevant project meetings feature security on the agenda - identifying likely attacks & designing necessary measures. During system maintenance, policy states potential breaches will be prevented by identifying unsuccessful attempts.

Employees are aware of their responsibilities to information security & a communal effort exists to notify any such breaches by an employee. Employee communication is liable to monitoring.

Investigating breaches of security

On identifying a successful breach, the Data controller with the relevant Manager will take the following actions:

- Take emergency measures to cease breach
- Investigate effects of breach
- Notify relevant parties of the extent
- Take measures to fix breach & prevent future attempts
- Reinstate system
- The Data Controller will hold a Senior Management meeting to determine whether the breach requires us to inform the ICO.

Integrity & Continuity

- User data kept up-to-date by subject by periodic review with prompt removal of inactive users
- Version control system in place for systems
- Centrally managed virus control system throughout network clients
- Nightly, weekly and monthly full backups to disk for entire server environment. Retained for 1 week, 1 month and 12 months respectively.
- Backup servers located in Griffin House and White Lion House for resilience.
- Backup system automatically notifies on failure and success
- Windows Previous Versions implemented on internal file servers, allows immediate recovery of accidentally altered files/documents.
- Externally hosted files subject to 3rd party backup systems & organised by IT Manager
- Periodic, manual backups of externally hosted files
- Externally hosted systems policies screened by IT Manager
- IT Contractors prepared to assist in disaster recovery hardware/configuration
- In the event of loss/failure of one building White Lion or Griffin House, the other can continue in isolation with regards to files/systems availability to users.

Staff Training

The organisation has policy to inform employees of the Data Security policies during induction and upon change. Senior Management prompt an annual “key point” training session.

Managing Director

1. Aims & Objectives:

The aim of this policy is to provide a framework to enable staff to understand:

1. The law regarding personal data

2. How personal data should be processed, stored, archived and deleted/destroyed

3. How staff can access personal data

1.1. Data Protection Principles

Anyone who processes personal information must comply with the six principles of the GDPR, which make sure that personal information is:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
4. 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 ('accuracy');
5. 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
6. 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 ('integrity and confidentiality').

2. Data Types

Not all data needs to be protected to the same standards, the more sensitive or potentially damaging the data is, the better it needs to be secured. There is inevitably a compromise between usability of systems and working with data. The DPA defines different types of data and prescribes how it should be treated. The loss or theft of any Personal Data is a "Potential Data Breach" which could result in legal action against the business. The loss of sensitive personal data is considered much more seriously and the sanctions may well be more punitive.

2.1. Personal data

AGD Systems has access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances.

This will include:-

- Personal information about employees e.g. names, addresses, contact details, D of B.
- Professional records e.g. employment history, taxation and national insurance records, appraisal records, disciplinary records and references
- Any other information that might be disclosed.

2.2. Sensitive Personal data

Sensitive personal data is defined by the Act as information that relates to the following 8 categories: race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexual life and biometric data. This requires a greater degree of protection and would include:-

- Medical information about a staff member.
- Information relating to any criminal offence of a member of staff.

2.3. Other types of Data not covered by the act.

This is data that does not identify a living individual and therefore is not covered by the remit of the GDPR AGD Systems may choose to protect some data in this category but there is no legal requirement to do so.

3. Responsibilities

The MD and Directors have overall responsibility for Data Protection.

- 3.1. Risk Management – Roles: Data Protection Officer AGD has nominated a member of staff responsible for the management of data protection. According to the ICO the minimum role will include:
- Informing and advising the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- Monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- Being the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

3.2. Risk management - Employee Responsibilities

Everyone at AGD has the responsibility of handling personal information in a safe and secure manner in compliance with the GDPR.

3.3. Risk Assessments

AGD will complete risk assessments for all data held.

4. Legal Requirements

4.1. Information for Data Subjects (Employees)

In order to comply with the fair processing requirements of the GDPR, AGD will inform employees of the data they collect, process and hold, the purposes for which the data is held and the third parties to whom it may be passed. Our Privacy Notice will be made available to all employees and provided within our website.

5. Transporting, Storing and Deleting Personal Data

The policy and processes of AGD will comply with the guidance issued by the ICO.

5.1. Information security - Storage and Access to Data

5.1.1. Technical Requirements

1. AGD will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system. Refer to the Information & Integrity Policy for more details.
2. Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for a period of time.
3. All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
4. Personal data can only be stored on AGD equipment (this includes computers and portable storage media (where allowed). Private equipment (i.e. owned by the users) must not be used for the storage of personal data.
5. The company has clear policy and procedures for the automatic backing up, accessing and restoring all data held on AGD Systems, including off-site backups. We fully understand the risk of data loss and the implications of a cyber attack.

5.1.2. Portable Devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

The data must be securely deleted from the device once it has been transferred or its use is complete.

5.1.3. Passwords

All users will use strong passwords which must be changed regularly. User passwords must never be shared. It is advisable NOT to record complete passwords, but prompts could be recorded.

5.1.4. Images

Images will be protected and stored in a secure area.

5.1.5. Cloud Based Storage

AGD has clear policy and procedures for the use of “Cloud Based Storage Systems” (for example Dropbox, Google apps and Google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the GDPR. AGD will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

5.2. Third Party data transfers

As a Data Controller, AGD is responsible for the security of any data passed to a “third party”. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party as well as data processing agreements.

5.3. Retention of Data

Personal data that is no longer required will be destroyed and this process will be recorded.

5.4. Systems to protect data

5.4.1. Paper Based Systems

All paper based personal data will be protected by appropriate controls, for example:

Paper based safeguarding chronologies will be in a locked cupboard when not in use

All Personal data will be disposed of by shredding

5.4.2. Websites

Uploads to the website will be checked prior to publication, for instance:

to check that appropriate photographic consent has been obtained

to check that the correct documents have been uploaded.

5.4.3. E-mail

E-mail cannot be regarded on its own as a secure means of transferring personal data.

Where technically possible all e-mails containing sensitive information will be encrypted by attaching the sensitive information as a word document and encrypting the document or password protecting. The recipient will then need to contact AGD for access to a one-off password.

6. Data Sharing

Where data that is shared, it is transmitted securely for instance by secure e-mail.

7. Data Breach – Procedures

On occasion, personal data may be lost, stolen or compromised. The data breach includes both electronic media and paper records, and it can also mean inappropriate access to information.

In the event of a data breach the Data Protection Officer will follow the procedures laid down in the Information Security & Integrity Policy.

8. Policy Review Reviewing:

This policy will be reviewed and updated if necessary annually or when legislation changes.

Managing Director

Statement of intent

Modern slavery is a crime and a violation of fundamental human rights. It takes various forms, such as slavery, servitude, forced and compulsory labour, and human trafficking, all of which include the deprivation of a person's liberty by another in order to exploit them for personal or commercial gain.

Policy Aims

AGD has a zero-tolerance approach to modern slavery within its business and supply chains.

This policy applies to all persons who act on our behalf in any capacity, including employees at all levels, directors, consultants, agency workers, and our supply chain.

AGD is committed to:

(a) acting ethically and with integrity in all our business dealings and relationships;

(b) implementing and enforcing effective systems and controls to ensure modern slavery is not taking place anywhere in our business or in any of our supply chains;

(c) ensuring there is transparency in our approach to tackling modern slavery in our business and in our supply chains consistent with our disclosure obligations under the Modern Slavery Act 2015.

We expect the same high standards from all of our Suppliers. As part of our contracting process, we include specific prohibitions against modern slavery, and we expect that our Suppliers will hold their own suppliers to the same high standards.

Managing Director