AARK DISPLAY LIMITED
DATA PROTECTION, DATA BREACH AND SOCIAL MEDIA POLICY

INTRODUCTION

PURPOSE

Aark Display Ltd is committed to being transparent about how it collects and uses the personal data of its employees, clients and associates, and to meeting its data protection obligations. This policy sets out Aark Display's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, associates, former employees, the personal data of clients and any other personal data processed for business purposes.

The organisation has appointed their CSR Lead to also lead for data protection and privacy notices. The CSR Lead's role is to inform and advise Aark Display Ltd on its data protection obligations. The CSR Lead can be contacted via email on hr@aarkdisplay.co.uk. Questions about this policy, or requests for further information, should be directed to Aark Display data protection lead.

DEFINITIONS

"Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data (for the purpose of uniquely identifying a person).

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

Aark Display Ltd processes personal data in accordance with the following data protection principles:

- The organisation processes personal data lawfully, fairly and in a transparent manner.
- The organisation collects personal data only for specified, explicit and legitimate purposes.
- The organisation processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The organisation keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The organisation keeps personal data only for the period necessary for processing.
- The organisation adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Aark Display Ltd tells employees, clients and associates the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. If the organisation wants to start processing data for other reasons, individuals will be informed of this before any processing begins.

Data will not be shared with third parties, except as set out in the privacy notices. Where the organisation relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where Aark Display Ltd processes special categories of personal data or criminal records data to perform obligations, to exercise rights in employment law, or for reasons of substantial public interest, this is done in accordance with the appropriate legislation regarding processing specialist categories of data and criminal records data.

Aark Display Ltd will update personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered during the employment relationship is held in hard copy and electronic format. The periods for which the organisation holds personal data are contained in its privacy notices to individuals.

The organisation keeps a record of its processing activities in respect of personal data in accordance with the requirements of the UK General Data Protection Regulation (UK GDPR).

INDIVIDUAL RIGHTS

As a data subject, individuals have a number of rights in relation to their personal data.

SUBJECT ACCESS REQUESTS

Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will tell them:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the UK and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the organisation has failed to comply with their data protection rights; and
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

The organisation will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically.

There will not normally be an associated charge for the completion of a subject access request , unless the request is deemed excessive or additional copies are requested. Any charges by the organisation will be based on the administrative cost to the organisation.

To make a subject access request, please contact the CSR Lead via email hr@aarkdisplay.co.uk. If you believe that the organisation has not complied with your data protection rights, you can complain to the Information Commissioner.

In some cases, the organisation may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify their identity and the documents it requires.
The organisation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the request is complex, it may respond within three months of the date the request is received. The organisation will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded if it is made with the intention of harassing the organisation or causing disruption, or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify them that this is the case and whether or not it will respond to it.

OTHER RIGHTS

Individuals have a number of other rights in relation to their personal data. They can require the organisation to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data.

To ask the organisation to take any of these steps, the individual should send the request to hr@aarkdisplay.co.uk

DATA SECURITY

The organisation takes the security of personal data seriously. The organisation has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees, clients and associates in the proper performance of their duties. Aark Display Ltd utilises an internal policy detailing the actions to be taken by the Aark Display data protection lead when a data breach is suspected.

Where the organisation engages third parties to process personal data on its behalf, such parties do so on the basis that the party are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Aark Display Consulting Limited adopts procedures designed to maintain the security of data when it is stored and transported.

In addition, employees must:

- Ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them.
- Ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people.
- Check regularly on the accuracy of data being entered into computers.
- Choose passwords with at least twelve characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.) Use a Password manager to generate unique and complex passwords.
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- It is mandatory to change passwords every thirty days. Passwords should not be reused, nor the same password used on multiple sites.
- It is mandatory to use multi-factor authentication in all accounts that support it.
- Avoid opening attachments and clicking on links when the content is not adequately explained, or from an unknown sender.
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

- If an employee isn't sure that an email, they received is safe, they can refer Aark Display's IT support team by forwarding the unopened email to helpdesk@r-i-t.com.
- Must not attempt to install unapproved spoftware on Aark Display Ltd's devices without prior permission from the IT Lead or a member of the senior management team.
- Must not perform any actions that disrupt or disable the managed installation of Windows updates and patch management
- Must not disable or attempt to disable device security measures including anti-virus or data protection services
- Confidential documents containing personal data should only be emailed when they are password protected and the password must be sent separately to the client via text message or encrypted WhatsApp message (i.e. a separate method of communication in the unlikely event that the email system becomes compromised).

Personal data relating to employees, clients and associates should not be kept or transported on laptops, USB sticks, or similar devices, unless there is a clear business need to do so. Where personal data is recorded on any such device it should be protected by:

- Ensuring that data is recorded on such devices only where absolutely necessary.
- Using an encrypted system or password protected document(s) — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted or password protected.
- Ensuring that laptops or USB drives are not left unsupervised in public areas where they can be lost or stolen.

Failure to follow these rules on data security may be dealt with via the Aark Display's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

DATA BREACHES

If the organisation discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The organisation will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

International data transfers

- No company data should be transferred outside the United Kingdom without prior authorisation by the IT Lead or a member of the senior management team.
- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary.
- Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorized people or organisations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts.
- Data should not be emailed, but when sharing internally in Aark Display it should be accessed via SharePoint and OneDrive. When sharing with a client, then it should be shared via MS Teams, with only the designated appropriate members having access.
- WhatsApp should not be used to send data between Aark Display and clients.
- If associates are audited as part of their coaching or other accreditation and need to share client names and emails as part of this process, they must let Aark Display know.

INDIVIDUAL RESPONSIBILITIES

Individuals are responsible for helping the organisation keep their personal data up to date. Individuals should let the organisation know if data provided to the organisation changes, for example if an individual moves house or changes bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, or when acting as an associate. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to staff, customers and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing it or that can be used to access personal data, without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to Kate Tomkin, the Aark Display data protection lead, immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

TRAINING

The organisation will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

DATA BREACHES

BREACH NOTIFICATIONS

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner (ICO) within 72 hours of Aark Display Ltd becoming aware of it. As information becomes clearer, it is permissible that the suspected data breach may be reported to the Information Commissioner in more than one instalment.

Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual. If the breach is sufficient to warrant notification to the public, the Company will do so without undue delay.

DATA BREACH NOTIFICATION POLICY

Aark Display is fully aware of its obligations under the UK General Data Protection Regulation (GDPR) to process data lawfully and to ensure it is kept securely. We take these obligations extremely seriously and have protocols in place to ensure that, to the best of our efforts, data is not susceptible to loss or other misuse. The GDPR incorporates a requirement for a personal data breach to be notified to the supervisory authority and in some cases to the affected individuals. This policy sets out the Company's stance on taking action in line with GDPR if a breach were to occur.

PERSONAL DATA BREACH

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed. A 'breach', for these purposes, is identifiable as a security incident which has affected the confidentiality, integrity or availability of personal data. As indicated above, a data breach for these purposes is wider in scope than the loss of data. The following are examples of data breaches:

- Access by an unauthorised third party.
- Deliberate or accidental action (or inaction) by a data controller or data processer.
- Sending personal data to an incorrect recipient.
- Computing devices containing personal data being lost or stolen.
- Alteration of personal data without permission.
- Loss of availability of personal data.

BREACH DETECTION MEASURES

We have implemented the following measures to assist us in preventing and detecting a personal data breach:

- Limited physical access to Aark Display IT systems and data.
- Password protection of Aark Display Ltd IT systems (computers and laptops).
- Password protected MS Office 360 email communications.
- Confidential documents sent password protected to clients via email.
- Passwords for confidential documents sent to clients are to be provided separately to the protected document utilising a SMS or WhatsApp message.
- Active and up-to-date anti-virus software support and monitoring is present on all Aark Display Ltd IT systems.

Aark Display Ltd may also become aware of a personal data breach from a member of staff, a client/customer, or a member of the public etc.

NOTIFIABLE BREACHES

For the purposes of this policy, a data breach will be notifiable when it is deemed by Aark Display Ltd as likely to pose a risk to people's rights and freedoms. If it does not carry that risk, the breach is not subject to notification although it will be entered on the Company's breach record. A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation. When assessing the likelihood of the risk to people's rights and freedoms, the Company will consider:

- The type of breach.
- The type of data involved including what it reveals about individuals.
- How much data is involved?
- The individuals involved e.g. how many are involved, how easy it is to identify them, whether they are children etc.
- How bad the consequences for the individuals would be?
- The nature of the Company's work and the resultant severity of a breach.

ACTIONS UPON IDENTIFICATION OF BREACH

When Aark Display Ltd is made aware of a breach, it will notify Resource Intelligent Technology by calling 0116 344064 and emailing helpdewsk@r-i-t.com to raise an incident for them to undertake an immediate investigation to ascertain the source of the breach and ensure the breach is no longer occurring. Thereafter, the investigation will identify what happened and what actions must be taken to restrict any consequences. A determination will be made at that point whether the breach is deemed a notifiable breach and whether it is deemed as resulting in a high risk to the rights and freedoms of individuals.

Aark Display's IT support company Resource Intelligent Technology need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists by raising a ticket by calling 0116 344064 and emailing helpdesk@r-i-t.com. Resource Intelligent Technology must investigate promptly, resolve the issue and send a companywide alert when necessary.

TIMESCALES FOR NOTIFICATION TO SUPERVISORY AUTHORITY

Where a notifiable breach has occurred, the Company will notify the ICO without undue delay and at the latest within 72 hours of it becoming aware of the breach. If notification is made beyond this timeline, the Company will provide the ICO with reasons for this.

If it has not been possible to conduct a full investigation into the breach in order to give full details to the ICO within 72 hours, an initial notification of the breach will be made within 72 hours, giving as much detail as possible, together with reasons for incomplete notification and an estimated timescale for full notification. The initial notification will be followed up by further communication to the ICO, where the submission of additional information is appropriate and/or necessary.

CONTENT OF BREACH NOTIFICATION TO THE SUPERVISORY AUTHORITY

The following information will be provided when a breach is notified:

- A description of the nature of the personal data breach including, where possible:
  - o The categories and approximate number of individuals concerned.
  - o The categories and approximate number of personal data records concerned.
- The name and contact details of the Data Protection Lead where more information can be obtained.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

TIMESCALES FOR NOTIFICATION TO AFFECTED INDIVIDUALS

Where a notifiable breach has occurred which is deemed to have a high risk to the rights and freedoms of individuals, the Company will notify the affected individuals themselves i.e. the individuals whose data is involved in the breach, in addition to the supervisory authority. This notification will be made without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified. A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

CONTENT OF BREACH NOTIFICATION TO THE AFFECTED INDIVIDUALS

The following information will be provided when a breach is notified to the affected individuals:

- A description of the nature of the breach.
- The name and contact details of the DPO where more information can be obtained.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

RECORD OF BREACHES

Aark Display records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under GDPR. It records the facts relating to the breach, its effects and the remedial action taken.

AARK DISPLAY CONSULTING DATA PROTECTION LEAD

Aark Display Ltd CSR lead can be contacted via email hr@aarkdisplay.co.uk

SOCIAL MEDIA

INTRODUCTION

This policy sets out our organisation's expectations on the workforce's use of social media and reminds staff of the standards of behaviour expected of them when they are posting on social media, as well as the consequences of falling below those standards.

This policy does not form part of your contract of employment, and we reserve the right to amend or withdraw it at any time.

SCOPE

For the purposes of this policy, social media is any online platform or app that allows parties to communicate instantly with each other or to share data in a public forum. This includes social forums such as X (formerly known as Twitter), Facebook and LinkedIn. Social media also covers blogs and video and image-sharing websites such as YouTube.

Employees should be aware that there are many more examples of social media than can be listed here and this is a constantly changing area. Employees should follow these guidelines in relation to any social media that they use.

This policy applies to employees. It does not apply to workers, contractors, consultants or any self-employed individuals working for the organisation.

USE OF SOCIAL MEDIA AT WORK

Employees are allowed to access social media from our organisation's computers or devices at certain times (provided that they are not undertaking overtime). Employees must limit their use of social media to their official rest breaks such as their lunch break/times when they are between [job, for example travelling/times when they are not on duty/times when they are not manning the telephones/times when they are not on the site where they are working.]

We understand that employees may wish to use their own computers or devices to access social media while they are at work. Employees must limit their use of social media on their own equipment to their official rest breaks such as their lunch break.

MONITORING USE OF SOCIAL MEDIA DURING WORK TIME

We reserve the right to monitor employees' use of social media on our organisation's equipment. We consider that valid reasons for checking an employee's internet usage include suspicions that the employee has:

- been using social media when they should be working; or
- acted in a way that is in breach of the rules set out in this policy.

Monitoring will consist of checking the social media sites that an employee has visited, the duration of such visits and the content that the employee has contributed on such sites.

[Monitoring will normally be conducted by our organisation's data security lead. The information obtained through monitoring may be shared internally, including with an employee's line manager, managers in the business area in which the employee works and IT staff if access to the data is necessary for performance of their roles. However, information would normally be shared in this way only if our organisation has reasonable grounds to believe that there has been a breach of the rules set out in this policy.

[The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted. Data is normally securely destroyed after [insert number of days/ weeks, depending on the reasons for monitoring]. We do not apply automated decision-making to the data obtained through monitoring.

Workers have a number of rights in relation to their data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances. You can find further details of these rights and how to exercise them in our organisation's data protection policy. If workers believe that our organisation has not complied with their data protection rights, they can complain to the Information Commissioner.

Access to particular social media may be withdrawn in any case of misuse.

SOCIAL MEDIA IN YOUR PERSONAL LIFE

Our organisation recognises that many employees make use of social media in a personal capacity. While they are not acting on behalf of our organisation, employees must be aware that they can damage our organisation if they are recognised as being one of our employees.

Employees are allowed to say that they work for our organisation, which recognises that it is natural for its staff sometimes to want to discuss their work on social media. However, the employee's online profile (for example, the name of a blog or an X name) must not contain our organisation's name.

If employees do discuss their work on social media (for example, giving opinions on their specialism or the sector in which our organisation operates), they must include on their profile a statement along the following lines: "The views I express here are mine alone and do not necessarily reflect the views of my employer."

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

- bring our organisation into disrepute, for example by:
  - criticising or arguing with customers, colleagues or rivals;
  - making defamatory comments about individuals or other organisations or groups; or
  - posting images that are inappropriate or links to inappropriate content;
- breach confidentiality, for example by:
  - revealing trade secrets or information owned by our organisation;
  - giving away confidential information about an individual (such as a colleague or customer contact) or organisation (such as a rival business); or
  - discussing our organisation's internal workings (such as deals that it is doing with a [customer/client] or its future business plans that have not been communicated to the public);

- breach copyright, for example by:
  - using someone else's images or written content without permission;
  - failing to give acknowledgment where permission has been given to reproduce something; or
- 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;
  - using social media to bully another individual (such as an employee of our organisation); or
  - posting images that are discriminatory or offensive [or links to such content].

USE OF SOCIAL MEDIA IN THE RECRUITMENT PROCESS

Unless it is in relation to finding candidates (for example, if an individual has put their details on social media websites for the purpose of attracting prospective employers), the HR department and managers should conduct searches, either themselves or through a third party, on social media only when these are directly relevant to the applicant's skills or claims that they have made in the recruitment process. For instance:

- a prospective employee might claim that they have used social media in their previous job (for example, as a publicity tool); or
- a prospective employee's social media use may be directly relevant to a claim made in their application (for example, if they run a blog based around a hobby mentioned in their CV or a skill in which they claim to be proficient).

There should be no systematic or routine checking of prospective employees' online social media activities, as conducting these searches during the selection process might lead to a presumption that an applicant's protected characteristics (for example, sexual orientation or religious beliefs) played a part in a recruitment decision. This is in line with our organisation's equal opportunities policy.]

DISCIPLINARY ACTION OVER SOCIAL MEDIA USE

All employees are required to adhere to this policy. Employees should note that any breaches of this policy may lead to disciplinary action. Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity that might cause serious damage to our organisation, may constitute gross misconduct and lead to summary dismissal.

Aark Display CSR lead
Aark Display Ltd

Reviewed: April 2025