General Data Protection Regulations (GDPR) policy

Purpose
As a data controller, VGC commits to being transparent about how we collect and use personal and sensitive data.

As a data controller, VGC is committed to being transparent about how it collects and uses personal and sensitive data and to meeting its data protection obligations under the General Data Protection Regulations (GDPR).

This policy applies to personal and sensitive data relating to job applicants, employees, workers contractors, former staff, clients and data processed for business purposes.

Ciara Pryce, group services director it the appointed data protection officer (DPO). Any GDPR queries or questions about this policy should be directed to Ciara Pryce at ciara.pryce@vgcgroup.co.uk

Definition of key terms
Personal data – any information that relates to a living individual who can be identified from that information.

Processing – any use of data, including collecting, storing, amending, disclosing or destroying it.

Sensitive data - information about a person's race or ethnic origin, religious or philosophical beliefs, trade union membership, physical and mental health, political opinions and sexual orientation.

Data controller - a person or organisation which decides on how and why personal data is processed

Data processor - the person or organisation which processes personal data on behalf of the data controller;

Data protection principles
VGC processes personal data in accordance with the following data protection principles:

- process personal data lawfully, fairly and in a transparent manner.
- collect data for specified and legitimate purposes, and not process data in a manner that is incompatible with those purposes.
- collect data that is adequate, relevant, and limited to what is necessary for the purposes of processing.
- ensure that data is accurate and kept up to date, and take every reasonable step to correct or delete data that is inaccurate without delay.
- keep data only as long as necessary for the purposes of processing.
- ensure that appropriate security is in place to protect data against unauthorised or unlawful processing, accidental loss, destruction or damage.
- process data in accordance with the rights of data subjects.

Legal bases for processing
VGC processes data for a number of reasons;

- to administer work-finding services for work seekers and clients.
- to meet statutory and contractual obligations such as wage payment and benefit and pension entitlements.
- to comply with legal obligations such as checking entitlement to work in the UK, HMRC deductions and health and safety laws.
- For certain positions, we must carry out criminal records checks to ensure that individuals are permitted to undertake the role in question.
- obtain occupational health advice, to comply with duties in relation to people with disabilities and to meet obligations under health and safety law.
- disclose personal data relating to a safety issue or breach of the RTAS scheme rules with the assurance organisation of the responsible team with the client.
- respond to and defend against legal claims
- maintain and promote equality in the workplace.
- implement high quality health and safety systems.

VGC will only process personal data where it has a legal basis. We will keep a register of our data processing activities, legal reasons for processing and retention periods in accordance with the requirements of the GDPR.

Where we rely on legitimate interests as the basis for processing data, we have checked that those interests are not overridden by the rights and freedoms of individuals.

We tell people why we are processing their personal data, how we use such it and the legal basis for processing.

Rights of data subjects
Data subjects have a number of rights in relation to their personal data.

- **Subject access requests**
  Please email the data protection officer if you want to ask for access to your personal data. VGC will respond to a request within 30 days from the date we receive the request. If you request large amount of data, we may extend the response period to within three months. We will write to the you within one month of receiving the original request to inform you of an extended response period.

- **Rectify inaccurate data**
  We will update your personal data promptly if you tell us that your information has changed or is inaccurate.

  If we have given the personal data to a third party e.g. a client, we will tell them to rectify your personal data unless this proves impossible or disproportionate. VGC will not be in a position to audit the third parties to ensure they have done this.

- **Erasure**
  You have the right to ask VGC to erase personal data. Please inform the data protection officer if you want us to remove your data completely, or to keep your details on a list of individuals not to be contacted.

  If you have asked to have your data erased completely we cannot keep a record that you do not wish to be contacted which may result in you being contacted by us at some time in the future.

  There may be reasons why we will still need to hold data e.g. for legal or official reasons such as legal claims. In this case we will tell you, and we will keep only what is necessary to meet those specific legal reasons

- **Restriction of processing**
  Individuals have the right to restrict the processing of personal data if;
  - it is believed to be inaccurate
  - the processing is unlawful and but you do not want it to be erased.
  - your personal data is no longer needed to be processed except for legal claims
  - you have objected to processing while it is decided if our legitimate grounds override yours.

- **Data portability**
  Individuals have the right to receive personal data that they have provided to VGC in a structured, commonly used and machine readable format. You have the right to request that VGC transmit this data directly to another data controller. If you do, we will send your personal data directly where possible.

- **Object to processing**
  You have the right to object to the processing or profiling of your personal data based on a public or a legitimate interest.

  If you do object, we will stop processing unless we have compelling legitimate grounds to continue to process the personal data, and these override your interests, rights and freedoms.

If you want to exercise these rights, send a written request to the data protection officer. We will act upon any request within one month of receipt of the request. VGC may extend this period for two further months where necessary, depending on the complexity and the number of requests.

If VGC considers that your request is manifestly unfounded or excessive due to the request's repetitive nature we may refuse to act on the request, or we may charge a reasonable fee taking into account the administrative costs involved.

Everyone has the following rights under the Human Rights Act 1998 (HRA) which we respect;

- Right to respect for private and family life
- Freedom of thought, belief and religion
- Freedom of expression
- Freedom of assembly and association
- Protection from discrimination in respect of rights and freedoms under the HRA

Data protection by design and by default

VGC takes the security of your data very seriously and has internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by data processors in the performance of their duties.

Organisational measures

- Appointment of data protection officer
- Departmental managers with day-to-day responsibility for data security measures i.e. ensuring filing cabinets are locked, data is not released without relevant disclosure signatures etc
- Policy on decommissioning and disposing of any IT equipment).
- Restricted access to premises or equipment given to anyone outside the organisation.
- Brief new and existing staff on data protection and security policy.
- External GDPR training and refresher training.
- Responsibility for protecting personal data included in job descriptions.
- Included in disciplinary procedure - including the possibility that they may commit criminal offences if they deliberately try to access, or to disclose, information without authority
- HR procedures on disclosing information to callers.

Technological

- Perimeter security – IPS, IDS firewall with advanced malware protection
- Email security – reputation based filtering, advanced malware protection, TLS enabled
- Endpoint security – all endpoints are encrypted and protected by advanced malware protection system.
- Storage – all the information data is encrypted at storage level.
- Endpoint encryption including mobile phones.
- Processes in place to protect and recover any personal data the organisation holds
- Periodic checks to ensure that the organisation's security measures remain appropriate and up to date.
- Monitoring of network activity i.e. websites being accessed, downloads of information, unauthorised access attempts.
- deploying a modern breach detection tools across our network to inform of any unauthorised attempt to access data and report on use of malware or malicious systems.
- IT training on how to detect hacking attempts and phishing.
- Staff training on the dangers of people trying to obtain personal data by deception, phishing attacks or by virus indection/spam.

Physical security:

- swipe card security.
- alarms.
- CCTV.
- Shredders and confidential waste bins.
- Computer security – malware detection, virus scanners.

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

VGC do not subject individuals to decisions based solely on automated decision-making.

Personal data breaches
We measures to protect personal data from incidents (either accidentally or deliberately) and avoid a data protection breach that could compromise security.

- Technological detection measures:
  - Maintaining secure systems through provision of the necessary infrastructure, resource and investment.
  - Monitoring of network activity i.e. websites being accessed, unauthorised access attempts, download of software onto computer systems.
  - Use of modern breach detection tools across our network to inform IT of any unauthorised attempt to access data, use of malware or malicious programmes.
  - Training on how to detect hacking attempts and phishing.
  - Procedures and policies in place for the decommission or loss of IT equipment.

- Management and organisational measures:
  - Appointment of a data protection officer responsible for data security measures.
  - Control measures are documented and communicated to staff at induction using relevant procedures and briefings.
  - Staff training on GDPR responsibilities and how to identify attacks, vulnerabilities and how to report.
  - Appointment of staff with accountability for monitoring departmental activities relating to personal data such as responsibility for ensuring data protection security measures are followed by staff and how to report suspected data breaches.

VGC will regularly review the technological and organisational measures put in place to assess effectiveness.

Any suspected breach will be fully investigated by the DPO. A deliberate or accidental action (or inaction) by a data controller or processor resulting in a data protection breach is a disciplinary offence and will be dealt with under our disciplinary procedure. It may be considered a gross misconduct offence and could lead to summary dismissal. A failure to report a suspected data breach may result in VGC's disciplinary procedure being instigated.

Where a breach occurs or is discovered outside normal working hours, it should be reported to the DPO as soon as is practicable. Once a data security incident has been reported, the DPO will assess the risk on a case by case basis taking into account the relevant factors and establish the likelihood and severity of the risk to people's rights and freedoms.

If it is assessed that the security incident will have an adverse effect on the individuals involved and has a high risk to their rights and freedoms, the DPO will report the personal data breach to individuals concerned and the relevant supervisory authority within 72 hours of the breach.

A record of the breach will be kept on a data security incident register.

Training
VGC will provide training to all individuals about their data protection responsibilities as part of the induction process.

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.

Complaints
If you believe that VGC has not complied with your data protection rights, you should inform the data protection officer in the first instance. You have the right to lodge any complaints to the information commission office (ICO) directly on 0303 123 1113.

Signed: Date: June 2019

Laurence Mckidd
Managing director