# General Data Protection Regulation
Portal Policies

Kabuki UK

# Kabuki UK
# GDPR Data Protection Policy

---

## 1. Scope

Kabuki UK and its management and Board of Sally Trewartha, Lisa Johnston, Beth Allen, with a registered address at 183 Englands Lane, Loughton, IG10 2NS are committed to being fully compliant with all applicable UK and EU data protection legislation in respect of personal data, as well to safeguarding the “rights and freedoms” of persons whose information Kabuki UK collects pursuant to the General Data Protection Regulation (“GDPR”) through the use of a Members Records Management System (“MRMS”), which is developed, implemented, maintained and periodically reviewed and amended by Kabuki UK’s Board of Directors.

The {{ MRMS shall take into consideration the following: organisational structure, management responsibility, jurisdiction and geographical location and may comprise of a defined part of Kabuki UK or Kabuki UK as a whole.

## 2. Objectives

Kabuki UK’s objectives for the MRMS are as follows:

1. To enable Kabuki UK to meet its personal data obligations in relation to how personal information is managed;

2. To support Kabuki UK’s objectives;

3. To set appropriate systems and controls according to Kabuki UK’s risk appetite;

4. To ensure that Kabuki UK is compliant with all applicable obligations, whether statutory, regulatory, contractual and/or professional; and

5. To safeguard personnel and stakeholder interests.

## 3. Good practice

Kabuki UK shall ensure compliance with data protection legislation and good practice, by at all times:

1. Processing personal information only when to do so is absolutely necessary for organisational purposes;

2. Ensuring that the least possible amount of personal data is collected, and that personal data is never processed unduly;

3. Informing individuals of how their personal data is or will be used and by whom;

4. Processing only pertinent and adequate personal data;

5. Processing personal data in a lawful and fair manner;

6. Keeping a record of the various categories of personal data processed;

7. Ensuring that all personal data that is kept is accurate and up-to-date;

8. Retaining personal data no longer than required by statute or regulatory body, or for organisational purposes;

9. Giving individuals the right of 'subject access', as well as all other individual rights pertaining to their personal data;

10. Ensuring that all personal data is maintained securely;

11. Transferring personal data outside of the EU only in situations where it shall be appropriately secured;

12. Applying various statutory exemptions, where appropriate;

13. Implementing a MRMS, pursuant to this Policy;

14. Identifying stakeholders, both internal and external, and ascertaining their involvement within the operation of the MRMS; and

15. Identifying personnel that are responsible and accountable for the MRMS.

**4. Notification**

Kabuki UK has registered with the Information Commissioner as a Data Controller' that engages in processing personal information of data subjects. Kabuki UK has identified all of the personal data that it processes and recorded it in its Data Inventory Schedule 92017-B.

The Data Controller shall retain a copy of all notifications made by
Kabuki UK to the Information Commissioner's Office ("ICO") Dropbox and the ICO Notification Handbook shall be used as a record of all notifications made.

The ICO notification shall be reviewed on an annual basis on 30.04.2018 and the Data Controller shall be responsible for each annual review of the details of the notification, keeping in mind any changes to Kabuki UK's activities. These changes shall be ascertained by reviewing the Data Inventory Schedule and the management review. Data protection impact assessments shall be used to ascertain any additional relevant requirements.

This policy applies to all employees of Kabuki UK, including contractors and subcontractors. Breaches of the GDPR policy, shall be dealt with according to Kabuki UK's Disciplinary Policy. If

there is a possibility that the breach could amount to a criminal offence, the matter shall be referred to the relevant authorities.

All third parties working with or for Kabuki UK who have or may have access to personal data are required to read, understand and fully comply with this policy at all times. All aforementioned third parties are required to enter into a data confidentiality agreement prior to accessing any personal data. The data protection obligations imposed by the confidentiality agreement shall be equally onerous as those to which Kabuki UK has agreed to comply with. Kabuki UK shall at all times have the right to audit any personal data accessed by third parties pursuant to the confidentiality agreement.

**5. GDPR background**

The purpose of the GDPR is to ensure the “rights and freedoms” of living individuals, and to protect their personal data by ensuring that it is never processed without their knowledge and, when possible, their consent.

**6. Definitions (as per the GDPR)**

- *Child* means anyone under the age of 16. It is only lawful to process the personal data of a child under the age of 13 upon receipt of consent from the child’s parent or legal custodian.

- *Data controller* may be a natural or legal person, whether a public authority, agency or other body which, individually or jointly with others, is in charge of ascertaining the purposes and means by which personal data shall be processed. Where EU or Member State law predetermines the purposes and means of processing personal data, the data controller or, if appropriate, the specific criteria for selecting the data controller, may be provided for by EU or Member State law.

- *Data subject* refers to any living person who is the subject of personal data (see above for the definition of ‘personal data’) held by an organisation. A data subject must be identifiable by name, ID, address, online identifier or other factors such as physical, physiological, genetic, mental, economic or social.

- *Data subject consent* refers to any specific indication by the data subject that signifies consent to the processing of personal data. Consent may take place by way of a written or oral statement or by clear, unambiguous action and must be given freely at all times, without duress, with the data subject being properly informed.

- *Establishment* refers to the administrative head office of the ‘data controller’ in the EU, where the main decisions regarding the purpose of its data processing activities are made. ‘Data controllers’ based outside of the EU are required to appoint a representative within the jurisdiction in which they operate to act on its behalf and liaise with the relevant regulatory and supervisory authorities.

- *Filing system* refers to any personal data set which is accessible on the basis of certain benchmarks, or norms and can be centralised, decentralised or dispersed across various locations.

- *Personal data* – means any information relating to a data subject.

- *Personal data breach* refers to a security breach which results in the disclosure, alteration, destruction or loss of personal data, as well as unauthorised access to personal data that is stored, transmitted or processed by any other means, whether accidentally or unlawfully. All personal data breaches must be reported to relevant regulatory authority by the 'data controller' at all times, whereas the data subject need only be informed of a data breach when it is likely that the breach will have an adverse effect on his or her privacy or personal data.

- *Processing* refers to any action taken in relation to personal data, including but not limited to collection, adaptation or alteration, recording, storage, retrieval, consultation, use, disclosure, dissemination, combination or deletion, whether by automated means or otherwise.

- *Profiling* refers to any form of personal data processing that is automated, with the intention of assessing personal aspects of a data subject or analysing a data subject's employment performance, economic status, whereabouts, health, personal preferences and behaviour. The data subject has a right to object to profiling and a right to be informed of the fact that profiling is taking place, as well as the intended outcome(s) of the profiling.

- *Special categories of personal data* refers to personal data covering such matters as racial or ethnic origin, beliefs - whether religious, political or philosophical - membership of a trade-union and data relating to genetics, biometric identification, health, sexual orientation and sex life.

- *Territorial scope* the GDPR applies to all EU based 'data controllers' who engage in the processing of data subjects**'** personal data as well as to 'data controllers' located outside of the EU that process data subjects**'** personal data so as to provide goods and services, or to monitor EU based data subject behaviour.

- *Third party* is a natural or legal person other than the data subject who is authorised to process personal data, whether a public authority, agency or other body controller, processor or any other person(s) under the direct authority of the controller or processor.

**7. Responsibilities under the GDPR**

Kabuki UK is a Data Controller pursuant to the GDPR.

Appointed employees of Kabuki UK with managerial or supervisory responsibilities are responsible for ensuring that good personal data handling practices are developed, reviewed and encouraged within Kabuki UK, as per their individual job descriptions.

*Data Controller*

The position of Data Controller which involves the management of personal data within Kabuki UK as well as compliance with the requirements of the DPA and demonstration of good practice protocol, is to be taken up by an appropriately qualified and experienced member of Kabuki UK's senior management team.

The Data Controller reports to Kabuki UK's Board of Directors and, amongst other things, is accountable for the development and implementation of the MRMS and for day-to-day compliance with this policy, both in terms of security and risk management. In addition, the Data Controller, is directly responsible for ensuring that Kabuki UK is GDPR compliant and that managers and executive officers of Kabuki UK are compliant in respect of data processing that occurs within their field of responsibility and/or oversight.

The Data Controller shall at all times be the first point of contact for any employees of Kabuki UK who require guidance in relation to any aspect of data protection compliance.

The Data Controller is also responsible for other procedures, such as the Subject Access Request Policy 92017-C.

It is not merely the Data Controller who is responsible for data protection, indeed all employees, volunteers, and sub-contractors of Kabuki UK who process personal data are responsible for ensuring compliance with data protection laws. Kabuki UK's GDPR Training Policy 92017-D provides for specific training for such, volunteers and sub-contractors (where appropriate) of Kabuki UK.

Employees, volunteers and sub-contractors of Kabuki UK are personally responsible for ensuring that all personal data they have provided and has been provided about them to Kabuki UK is accurate and up-to-date.

*Risk Assessment*

It is vital that Kabuki UK is aware of all risks associated with personal data processing and it is via its risk assessment process that Kabuki UK is able to assess the level of risk. Kabuki UK is also required to carry out assessments of the personal data processing undertaken by other organisations on its behalf and to manage any identified risks, so as to mitigate the likelihood of potential non-compliance with this policy.

Where personal data processing is carried out by using new technologies, or when a high risk is identified in relation to the "rights and freedoms" of natural persons, Kabuki UK is required to engage in a risk assessment of the potential impact. More than one risk may be addressed in a single assessment (also known as a 'Data Protection Impact Assessment' ("DPIA")).

If the outcome of a DPIA points to a high risk that Kabuki UK's intended personal data processing could result in distress and/or may cause damage to data subjects, it is up to the Data Controller to decide whether Kabuki UK ought to proceed and the matter should be

escalated to him or her. In turn, the Data Controller may escalate the matter to the regulatory authority if significant concerns have been identified.

It is the role of the Data Controller to ensure that appropriate controls are in place to ensure that the risk level associated with personal data processing is kept to an acceptable level, as per the requirements of the GDPR and Kabuki UK's documented risk acceptance criteria.

**8. Principles of data protection**

The principles of personal data processing are as follows:

1. All personal data must be processed lawfully and fairly at all times, as per Kabuki UK's Fair Processing Policy 92017-E.

2. Policies must also be transparent, meaning that Kabuki UK must ensure that its personal data processing policies, as well as any specific information provided to a data subject, are readily available, easily accessible and clear, drafted using clear and plain language.

3. The data subject must be provided with the following information:

    a. *Controller* - the identity and contact details of the Data Controller and any of its representatives;

    b. *Purpose* - the purpose or purposes and legal basis of processing;

    c. *Storage period* - the length of time for which the data shall be stored;

    d. *Rights* - confirmation of the existence of the following rights:
        i. Right to request access;
        ii. Right of rectification;
        iii. Right of erasure; and the
        iv. Right to raise an objection to the processing of the personal data;

    e. *Categories* - the categories of personal data;

    f. *Recipients* - the recipients and/or categories of recipients of personal data, if applicable;

    g. *Location* - if the controller intends to make a transfer of personal data to a third country and the levels of data protection provided for by the laws of that country, if applicable; and

    h. *Further information* - any further information required by the data subject in order to ensure that the processing is fair and lawful.

4. Personal data may only be collected for specified, explicit and legitimate reasons. When personal data is obtained for specific purposes, it must only be used in relation to that

purpose and cannot be different from the reasons formally notified to the Information Commissioner, as part of Kabuki UK's GDPR ICO registration.

5. Personal data must be adequate, relevant and restricted to only what is required for processing. In relation to this, the Data Controller shall at all times:

   a. Ensure that personal data which is superfluous and not necessarily required for the purpose(s) for which it is obtained, is not collected;

   b. Approve all data collection forms, whether in hard-copy or electronic format;

   c. Carry out an annual review of all methods of data collection, checking that they are still appropriate, relevant and not excessive; and

   d. Securely delete or destroy any personal data that is collected in a manner that is excessive or unnecessary according to Kabuki UK's GDPR policies.

6. Personal data must be accurate and up-to-date:

   a. Data should not be kept unless it is reasonable to assume its accuracy and data that is kept for long periods of time must be examined and amended, if necessary;

   b. All staff must receive training from the Kabuki UK's Head of HR to ensure they fully understand the importance of collecting and maintaining accurate personal data;

   c. Individuals are personally responsible for ensuring that the personal data held by Kabuki UK is accurate and up-to-date. Kabuki UK will assume that information submitted by individuals via data collection forms is accurate at the date of submission;

   d. All employees of Kabuki UK are required to update the HR department as soon as reasonably possible of any changes to personal information, to ensure records are up-to-date at all times;

   e. The Data Controller must ensure that relevant and suitable additional steps are taken to ensure that personal data is accurate and up-to-date;

   f. The Data Controller shall, on an annual basis, carry out a review of all personal data controlled by Kabuki UK, referring to the Data Inventory Register and ascertain whether any data is no longer required to be held in accordance with the guidelines of the ICO, arranging for that data to be deleted or destroyed in a safe manner.

   g. The Data Controller shall also ensure that where inaccurate or out-of-date personal data has been passed on to third parties, that the third parties are duly informed and instructed not to use the incorrect or out-of-date information as a means for making decisions about the data subject involved. The Data Controller shall also provide an update to the third party, correcting any inaccuracies in the personal data.

7. The form in which the personal data is stored must such that the data subject can only be identified when it is necessary to do so for processing purposes. The following principles apply:

   a. Personal data that is kept beyond the processing date must be either deleted, encrypted, pseudonymised or put beyond use and kept to an absolute minimum, to ensure the protection of the data subject's identity should a data breach incident occur;

   b. Personal data must be retained according to the Retention Requirements Policy 2017-F and must be destroyed or deleted in a secure manner as soon as the retention date has passed; and

   c. Should any personal data be required to be retained beyond the retention period set out in the Records Retention Procedure, this may only be done with the express written approval of the Data Controller, which must be in line with data protection requirements.

8. The processing of personal data must always be carried out in a secure manner.

9. Personal data should not be processed in an unauthorised or unlawful manner, nor should it be accidentally lost or destroyed at any time and Kabuki UK shall implement robust technical and organisational measures to ensure the safeguarding of personal data.

**9. Security controls**

Security controls are necessary to ensure that risks to personal data identified by Kabuki UK are appropriately mitigated as much as possible to reduce the potential for damage or distress to data subjects whose personal data is being processed and are subject to regular audit and review. Please refer to Kabuki UK's Security Access Policy 92017-G

Personal data shall not be transferred to a country outside of the EU unless the country provides appropriate protection of the data subject's 'rights and freedoms' in relation to the processing of personal data.

**10. Adequacy of transfer**

The following safeguards and exceptions are in place to ensure that data is not transferred to a country outside of the EU, with the transfer being off limits, unless one or more of the safeguards or exemptions listed below apply:

*Safeguards*

1. Assessing the adequacy of the transfer, by reference of the following:

   - The nature of the personal data intended to be transferred;
   - The country of origin and country of intended destination;
   - The nature and duration of the personal data use;

- The legislative framework, codes of practice and international obligations of the data subject's country of residence; and
- (UK only) the security measures to be implemented in the country of intended destination in relation to the personal data.

2. Binding corporate rules

Kabuki UK is free to implement approved binding corporate rules in relation to personal data transfer outside of the EU, however only with prior permission from the relevant regulatory body.

3. Model contract clauses

Kabuki UK is free to implement model contract clauses in relation to personal data transfer outside of the EU and there will be an automatic recognition of adequacy of transfer, should the model contract clauses receive approval from the relevant regulatory body.

*Exceptions*

In the absence of an adequacy decision, including binding corporate rules and model contract clauses, no transfer of personal data to a third country may take place unless one of the following preconditions is satisfied:

1. Explicit consent has been provided by a fully informed data subject, who has been made aware of all possible risks involved in light of appropriate safeguards and an adequacy decision;

2. The personal data transfer is a prerequisite to the performance of a pre-existing contract between the data controller and the data subject or when the data subject requests that pre-contractual measures are implemented;

3. The personal data transfer is a prerequisite to the conclusion or performance of a pre-existing contract between the data controller and another person, whether natural or legal, if it is in the interest of the data subject;

4. The personal data transfer is in the public interest;

5. The personal data transfer is required for the creation, exercise or defence of legal claims;

6. The data subject is not capable of giving consent, whether due to physical or legal limitations or restrictions and the personal data transfer is necessary for the protection of the key interests of the data subject or of other persons;

7. The personal data transfer is made from an approved register, confirmed by EU or Member State law as having the intention of providing public information and which is open to consultation by the public or by an individual demonstrating a legitimate interest, but only so far as the legal requirements for consultation are fulfilled.

## 11. Accountability

According to the GDPR accountability principle, the data controller is responsible both for ensuring overall compliance with the GDPR and for demonstrating that each of its processes is compliant with the GDPR requirements. To this extent data controllers are required to:

- Maintain all relevant documentation regarding its processes and operations;
- Implement proportionate security measures;
- Carry out Data Processing Impact Assessments (“DPIAs”);
- Comply with prior notification requirements;
- Seek the approval of relevant regulatory bodies; and
- Appoint a DPO where required.

## 12. The rights of data subjects

Data subjects enjoy the following rights in relation to personal data that is processed and recorded:

1. The right to make access requests in respect of personal data that is held and disclosed;

2. The right to refuse personal data processing, when to do so is likely to result in damage or distress;

3. The right to refuse personal data processing, when it is for direct marketing purposes;

4. The right to be informed about the functioning of any decision-making processes that are automated which are likely to have a significant effect on the data subject;

5. The right not to solely be subject to any automated decision making process;

6. The right to claim damages should they suffer any loss as a result of a breach of the provisions of the GDPR;

7. The right to take appropriate action in respect of the following: the rectification, blocking and erasure of personal data, as well as the destruction of any inaccurate personal data;

8. The right to request that the ICO carry out an assessment as to whether any of the provisions of the GDPR have been breached;

9. The right to be provided with personal data in a format that is structured, commonly used and machine-readable;

10. The right to request that his or her personal data is sent to another data controller; and

11. The right to refuse automated profiling without prior approval.

**13. Data access requests**

Subject Access Request Policy 92017-C sets out the procedure for making data access requests to data subjects and outlines how Kabuki UK will comply with the requirements of the GDPR regarding this.

**14. Complaints**

All complaints about the Kabuki UK's processing of personal data may be lodged by a data subject directly with the Data Controller, by filling in the appropriate form providing details of the complaint. The data subject must be provided with the organisations Privacy Policy at this stage.

Complaints may also be made by a data subject directly to the relevant regulatory body and Kabuki UK hereby provides the relevant contact details Sally Trewartha.

All complaints in relation to how a complaint has been handled and any appeals following the submission of a complaint shall be dealt with by the Data Controller and the data subject is required to submit a further complaint.

**15. Consent**

Consent to the processing of personal data by the data subject must be:

- Freely given and should never be given under duress, when the data subject is in an unfit state of mind or provided on the basis of misleading or false information;
- Explicit;
- Specific;
- A clear and unambiguous indication of the wishes of the data subject;
- Informed;
- Provided either in a statement or by unambiguous affirmative action;
- Demonstrated by active communication between the data controller and the data subject and must never inferred or implied by omission or a lack of response to communication;
- In relation to sensitive data, consent may only be provided in writing, unless there is an alternative legitimate basis for the processing of personal data.

*Employees*

Kabuki UK will obtain consent to process personal and sensitive data when a new employee signs an employment contract or during induction programmes. Data subjects have the right to withdraw consent at any time and have been notified via the on-boarding procedure of Kabuki UK.

Existing employees have been asked for their consent for Kabuki UK to process their personal and sensitive data

Employees have been notified of their rights under the GDPR within Kabuki UK's employee handbook.

Employees have been notified of their obligations under the GDPR within Kabuki UK's employee handbook.

*Other data subjects – Customers, supporters or members*
If using Consent as a condition to process data Kabuki UK will obtain Consent in accordance with the procedures outlined in the policy framework. Consent is considered to be a positive action on behalf of the data subject having read a clear, transparent and unambiguous privacy notice. It does not necessarily have to be a box that is ticked, it could be the completion of a form, or the supply of contact information. We understand that according to PECR consent does not have to be explicit. We will use our judgement to decide how to obtain consent in different circumstances. However, we will always uphold the rights and freedoms of data subjects by always making it as easy to Opt-out as it ever was to Opt-in.
We mostly use Consent when promoting the aims and objectives of our organisation, Kabuki UK. We reserve the right to use it wherever we believe a data subject has indicated their wishes and where we have collected the data for that particular purpose. We only use data for the purpose for which it was collected.

*Parental consent*

Parental or custodial consent is required if/when Kabuki UK is a provider of online services to children, defined as being under the age of 16.

**16. Data security**

All employees of Kabuki UK are personally responsible for keeping secure any personal data held by Kabuki UK for which they are responsible. Under no circumstances may any personal data be disclosed to any third party unless Kabuki UK has provided express authorisation and has entered into a confidentiality agreement with the third party.

*Accessing and storing personal data*

Access to personal data shall only be granted to those who need it and only according to the principles of the Kabuki UK's Access Policy 92017 G.

All personal data must be stored:
- In a locked room, the access to which is controlled; and/or
- In a locked cabinet, drawer or locker; and/or
- If in electronic format and stored on a computer, encrypted according to the corporate requirements set out in the Access Control Policy; and/or

- If in electronic format and stored on removable media, encrypted as per Disposal of Removable Storage Media 92017-H

Before being granted access to any organisational data, all staff of Kabuki UK must understand and have a copy of Access Policy 92017 G.

Computer screens and terminals must not be visible to anyone other than staff of Kabuki UK with the requisite authorisation.

No manual records may be accessed by unauthorised employees of Kabuki UK and may not be removed from the business premises in the absence of explicit written authorisation. Manual records must be removed from secured archiving when access is no longer needed on a day-to-day basis.

All deletion of personal data must be carried out in accordance with Kabuki UK's Retention Requirements 92017-F. Manual records which have passed their retention date must be shredded and disposed of as 'confidential waste' and any removable or portable computer media such as hard drives as USB sticks must be destroyed as per Disposal of Removable Storage Media 92017-H Policy prior to disposal.

Personal data that is processed 'off-site' must be processed by authorised Kabuki UK staff, due to the increased risk of its loss, damage or theft.

**17. Data access rights**

Data subjects have the right to access all personal data in relation to them held by Kabuki UK, whether as manual records or electronic format. Data subjects therefore may at any time request to have sight of confidential personal references held by Kabuki UK as well as any personal data received by Kabuki UK from third-parties. To do so, a data subject must submit a Subject Access Request, as per Subject Access Request SAR Form 92017-U.

**18. Disclosure of data**

Kabuki UK must take appropriate steps to ensure that no personal data is disclosed to unauthorised third parties. This includes friends and family members of the data subject, governmental bodies and, in special circumstances, even the Police. All employees of Kabuki UK are required to attend specific training in order to learn how to exercise due caution when requested to disclose personal data to a third party.

Disclosure is permitted by the GDPR without the consent of the data subject under certain circumstances, namely:

- In the interests of safeguarding national security;
- In the interests of crime prevention and detection which includes the apprehension and prosecution of offenders;
- In the interests of assessing or collecting a tax duty;
- In the interests of discharging various regulatory functions, including health and safety;
- In the interests of preventing serious harm occurring to a third party; and

- In the interests of protecting the vital interests of the data subject i.e. only in a life and death situation.

The Data Controller is responsible for handling all requests for the provision of data for these reasons and authorisation by the Data Controller shall only be granted with support of appropriate documentation.

**19. Data retention and disposal**

Kabuki UK must not retain personal data for longer than is necessary and once an employee has left Kabuki UK, it may no longer be necessary for Kabuki UK to retain all of the personal data held in relation to that individual. Some data will be kept longer than others, in line with Kabuki UK's data retention and disposal procedures in Disposal of Removable Storage Media 92017-H policy.

Personal data must be disposed of according to Kabuki UK's secure disposal procedure Disposal of Removable Storage Media 92017-H, to ensure that the "rights and freedoms" of data subjects it protected at all times.

**20. Document owner**

The Data Controller is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated 30.04.2018 is available to all employees of Kabuki UK on the corporate intranet.

This policy document was approved by Kabuki UK's Board of Sally Trewartha, Lisa Johnston, Beth Allen and is issued by the Chief Executive Officer ("CEO") on a version controlled basis.

Name of CEO: Sally Trewartha Date: 30.04.2018

**Change history record**

| Issue | Description of Change | Approval | Date of Issue |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |

# Kabuki UK
# Disposal of Removable Storage Media

## 1. Scope

This procedure covers all situations involving the disposal of removable storage media. Kabuki UK must ensure that all removable storage media are cleaned before being disposed of.

## 2. Responsibilities

It is the responsibility of Kabuki UK's Security Manager to manage the secure disposal of all storage media that is no longer required, according to this procedure. The Security Manager is also the owner of the relationship with the approved third party contractor who removes shredded documents.

All owners of removable storage media are responsible for disposing of removable storage media according to this procedure.

## 3. Procedure

1. Hard disks must be formatted and cleaned of all data and software before being reused or disposed of.

2. The secure disposal of disposable storage media as well as the disposal of all data processing equipment is the responsibility of the Information Security Manager.

3. The Information Security Manager shall keep a log demonstrating what media has been destroyed or disposed of, when and by whom 183 Englands lane, Loughton, IG10 2NS.

4. Hard disks must be cleaned and verified by taking the following steps: Delete information, empty trash on the computer.

5. If hard disks are cleaned and guaranteed by an external third party, then the details of the external service provider must be entered here .

6. Removable storage media devices that contain confidential information must be destroyed only after a risk assessment has been carried out and must never be reused.

7. Removable storage media devices that contain confidential information must be subjected to a risk assessment before they are sent for repair in order to establish whether they ought to be repaired or replaced.

8. The protocol for destroying removable storage media devices prior to disposal is as follows: .

9. All media must be disposed of according to the legal and regulatory requirements for the disposal of computer equipment, via If necessary company TBC, Kabuki UK's approved.

10. Documents that contain confidential and restricted information should be shredded by their owners prior to being destroyed. Shredders are located We have no paper records but if necessary company TBC. The shredded waste must be removed by an approved service provider, We have no paper records but if necessary company TBC.

**4. Document owner**

The Sally Trewartha is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated 30.04.2018 is available to all employees of Kabuki UK on the corporate intranet.

This policy document was approved by Kabuki UK's Board of Sally Trewartha, Lisa Johnston, Beth Allen and is issued by the Chief Executive Officer ("CEO") on a version controlled basis.

Name of CEO: Sally Trewartha Date: 30.04.2018

**Change history record**

| Issue | Description of Change | Approval | Date of Issue |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |

# Kabuki UK
# Security Access Policy

Kabuki UK will establish specific requirements for protecting information and information systems against unauthorised access.

Kabuki UK will effectively communicate the need for information and information system access control.

## 1 Purpose

Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of Kabuki UK which must be managed with care. All information has a value to the organisation. However, not all of this information has an equal value or requires the same level of protection.

Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use.

Formal procedures must control how access to information is granted and how such access is changed.

This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

## 1 Scope

This policy applies to all Kabuki UK 's Directors, Departments, Partners, and Employees (including system support staff with access to privileged administrative passwords), contractual third parties and agents of the organisation with any form of access to Kabuki UK 's information and information systems.

## 2 Definition

Access control rules and procedures are required to regulate who can access Kabuki UK information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing
Kabuki UK information in any format, and on any device.

## 3 Risks

On occasion business information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies, without the correct authorisation and clearance may intentionally or accidentally gain unauthorised access to business information which may adversely affect day to day business. This policy is intended to mitigate that risk.

Non-compliance with this policy could have a significant effect on the efficient operation of the organisation and may result in a breach of data, financial loss and an inability to provide necessary services to our customers**.**

# 4 Applying the Policy - Passwords

## 4.1 Choosing Passwords

Passwords are the first line of defence for our ICT systems and together with the user ID help to establish that people are who they claim to be.

A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

### 4.1.1 *Weak* and *strong* passwords

A *weak password* is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

A *strong password* is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

Everyone must use strong passwords with a minimum standard of:

- At least seven characters.
- Contain a mix of alpha and numeric, with at least one digit
- More complex than a single word (such passwords are easier for hackers to crack).

## 4.2 Protecting Passwords

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times [amend list as appropriate]:

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different Kabuki UK systems.
- Do not use the same password for systems inside and outside of work.

## 4.3 Changing Passwords

All user-level passwords must be changed at a maximum of every 90 days, or whenever a system prompts you to change it. Default passwords must also be changed immediately. If you become aware, or suspect, that your password has become known to someone else, you **must** change it immediately and report your concern to the trustees.

Users **must not** reuse the same password within password changes.

## 4.4 System Administration Standards

The password administration process for individual Kabuki UK  systems is well-documented and available to designated individuals.

All Kabuki UK  IT systems will be configured to enforce the following:

- Authentication of individual users, not groups of users - i.e. no generic accounts.
- Protection with regards to the retrieval of passwords and security details.
- System access monitoring and logging - at a user level.
- Role management so that functions can be performed without sharing passwords.
- Password admin processes must be properly controlled, secure and auditable.

# 5 Applying the Policy – Employee Access

## 5.1 User Access Management

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access.  They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. These must be agreed by Kabuki UK .  Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated.  System administration accounts must only be provided to users that are required to perform system administration tasks.

## 5.2 User Registration

A request for access to the organisation's computer systems must first be submitted to the the trustees.

When an employee leaves the organisation, their access to computer systems and data must be suspended at the close of business on the employee's last working day.  It is the responsibility of the the trustees to request the suspension of the access rights via the the trustees.

## 5.3 User Responsibilities

It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to the organisations systems by:

- Following the Password Policy Statements outlined above in Section 6.
- Ensuring that any PC they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing the trustees of any changes to their role and access requirements.

### 5.4 Network Access Control

The use of USB's and Remote LogIn methods on non-organisation owned PC's connected to the organisation's network can seriously compromise the security of the network. The normal operation of the network must not be interfered with. Specific approval must be obtained from the trustees before connecting any equipment to Kabuki UK's network.

### 5.5 User Authentication for External Connections

Where remote access to the Kabuki UK network is required, an application must be made via the the trustees. Remote access to the network must be secured by two factor authentication consisting of a username and one other component.

### 5.6 Supplier's Remote Access to the Organisations Network

Partner agencies or 3rd party suppliers must not be given details of how to access the organisations network without permission from the trustees. Any changes to supplier's connections must be immediately sent to the trustees so that access can be updated or ceased. All permissions and access methods must be controlled by the trustees.

Partners or 3rd party suppliers must contact the the trustees before connecting to the Kabuki UK network and a log of activity must be maintained. Remote access software must be disabled when not in use.

### 5.7 Operating System Access Control

Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section (section 7.1) and the Password section (section 6) above must be applied. The login procedure must also be protected by:

- Not displaying any previous login information e.g. username.
- Limiting the number of unsuccessful attempts and locking the account if exceeded.
- The password characters being hidden by symbols.
- Displaying a general warning notice that only authorised users are allowed.

All access to operating systems is via a unique login id that will be audited and can be traced back to each individual user. The login id must not give any indication of the level of access that it provides to the system (e.g. administration rights).

System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

### 5.8 Application and Information Access

Access within software applications must be restricted using the security features built into the individual product. The access must:

- Be compliant with the User Access Management section (section 7.1) and the Password section (section 6) above.
- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.

- Be unable to be overridden (with the admin settings removed or hidden from the user).
- Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.
- Be logged and auditable.

## 6 Policy Compliance

If any user is found to have breached this policy, they may be subject to Kabuki UK disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the trustees.

## 7 Policy Governance

The following table identifies who within Kabuki UK is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

| | |
|---|---|
| **Responsible** | the trustees |
| **Accountable** | the trustees |
| **Consulted** | the trustees |
| **Informed** | the trustees |

## 8 Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by n/a.

**Change history record**

| Issue | Description of Change | Approval | Date of Issue |
|---|---|---|---|
| 1 | n/a | n/a | n/a |
| 2 | n/a | n/a | n/a |
| 3 | n/a | n/a | n/a |

# Kabuki UK
# Subject Access Request Procedure

## 1. Scope

This procedure covers all personal data that is processed by Kabuki UK with the exception of personal data that is routinely requested by data subjects.

It is the right of all data subjects to ask Kabuki UK the following:

1. What personal data Kabuki UK is being processed about that person, if any;

2. To be provided with a description of the personal data processed Kabuki UK about that person;

3. The purpose or purposes for which the personal data is being processed;

4. Confirmation of who will have access to the personal data; and

5. To be provided with a copy of the personal data, as well as a confirmation of where Kabuki UK acquired that personal data.

## 2. Responsibilities

The Data Protection Officer (“DPO”) shall be responsible for the application and functionality of this procedure and shall handle all Subject Access Requests (“SARs”). The DPO shall report to the Head of IT on all matters relating to SARs.

## 3. Procedure

All SARs are made using form Subject Access Request Form 92017-C.

The data subject is required to provide evidence of his or her identity by way of a current passport or driving license and his or her signature must be cross-referenced with the signature provided on the Subject Access Request form.

The following information must be provided by the data subject on the Subject Access Request Form: the personal data that is being requested, whether specific data or all data held by Kabuki UK and where it is being held.

Kabuki UK is required to record the date on which the Subject Access Request Form, with the accompanying identification evidence, is submitted.

Kabuki UK has one month from this date to provide to the data subject the personal data requested. Should Kabuki UK fail to provide the requested information within the one month window, this shall be in direct breach of the GDPR. No extension shall be allowed under any circumstances.

It is vital that the Subject Access Form is sent to the DPO straight away, to ensure that the requested data is collected within the one month window.

The DPO will carry out data collection by one of the following steps:

1. Collecting the personal data requested; or

2. Carrying out a search of all electronic and hard-copy databases including manual files, backup and archived files as well as email folders and archives.

The DPO shall at all times have access to a data map which sets out the location of all of Kabuki UK's stored data.

At no time may personal data ever be altered or destroyed in order to avoid disclosure.

*Responsibilities*

The DPO is responsible for the following:

1. Keeping a record of all SARs made, including the date on which the SAR was received;

2. Reviewing all the documents provided to a data subject pursuant to a SAR to check for the mention of any third parties and if a third party is mentioned, to prevent the disclosure of the identity of the third party to the data subject, or to seek written consent from the third party as to the disclosure of their identity.

*Personal data exemption categories*

The following data exemption categories apply, meaning that Kabuki UK does not have to provide personal data covered below:

- The prevention and detection of crime;
- Negotiations with the data subject request maker;
- Management forecasts;
- Confidential references provided *by* Kabuki UK however not references provided *to* Kabuki UK
- Data covered by legal professional privilege;
- Data used for research, statistical or historical reasons.

Personal data provided by Kabuki UK to a data subject pursuant to a SAR shall be in electronic format, unless the SAR expressly requests otherwise and all items shall be scheduled, displaying the data subject's name and the date on which the data item was delivered.

**4. Document owner**

The Data Processor is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated {{ insert_date}} is available to all employees of Kabuki UK on the corporate intranet.

This policy document was approved by Kabuki UK's Board of Sally Trewartha, Lisa Johnson, Beth Allen and is issued by the Chief Executive Officer ("CEO") on a version controlled basis.

Name of CEO: Sally Trewartha Date: 30.04.2018

**Change history record**

| Issue | Description of Change | Approval | Date of Issue |
|---|---|---|---|
| 1 | n/a | n/a | n/a |
| 2 | n/a | n/a | n/a |
| 3 | n/a | n/a | n/a |

# Kabuki UK
# GDPR Training Policy

## 1. Specific training

Kabuki UK is responsible for ensuring that all employees who are responsible, on a day-to-day basis, for compliance with the General Data Protection Regulation ("GDPR") and relevant good practice, are able to exhibit competency in their understanding of the GDPR, good practice and the implementation thereof by Kabuki UK.

All persons with GDPR responsibility shall receive appropriate training and all training records are to be maintained by Kabuki UK's HR Department.

Kabuki UK shall also be responsible for ensuring that all persons with GDPR responsibility are regularly informed of and updated on all relevant matters related to personal data management, including through contact with external bodies, the most noteworthy of which is the Information Commissioner's Office (www.ico.gov.uk). Kabuki UK shall keep a list of all relevant external bodies for reference at all times.

## 2. General training

Kabuki UK is responsible for ensuring that all of its employees are aware of their personal responsibilities in relation to personal data, ensuring that it is properly protected at all times and is processed only in line with Kabuki UK's procedures.

To this end, Kabuki UK shall ensure that all of its employees are given appropriate and relevant training. It shall be the duty of Kabuki UK's HR Department to organise both specific training for GDPR responsible persons as well as general training for all staff and to maintain records of attendance.

## 3. Document owner

The Data Processor is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated {{ insert_date}} is available to all employees of Kabuki UK on the corporate intranet.

This policy document was approved by Kabuki UK's Board of The Trustees and is issued by the Chief Executive Officer ("CEO") on a version controlled basis.

Name of CEO: Sally Trewartha Date: 30.04.2018

**Change history record**

| Issue | Description of Change | Approval | Date of Issue |
|---|---|---|---|
| 1 | n/a | n/a | {{ insert_date_1 }} |
| 2 | n/a | n/a | n/a |
| 3 | n/a | n/a | n/a |

# Kabuki UK
# Fair Processing Procedure

---

## 1. Scope

The scope of this procedure encompasses all information processing of data subjects by Kabuki UK.

## 2. Fair Processing Notice

Responsibility for the Fair Processing Notice rests with the Data Protection Officer or GDPR Owner (hereafter “DPO”), who must ensure that it is factually correct and that appropriate mechanisms are in place to ensure that all data subjects are aware of its contents prior to the commencement of Kabuki UK’s data collection.

## 3. Procedure

Personal data may only be processed upon receipt of authorisation from the DPO.

The following information must be provided to data subjects prior to data collection, in plain and clear language:

1. Organisation Name, including contact details;

2. Objective behind the processing of personal information;

3. Duration of time the personal data will be stored for and the storage criteria;

4. Statement regarding the disclosure of personal information to third parties;

5. Information regarding the rights of data subjects in respect of their personal data, including but not limited to:
    - The right to access personal information;
    - The right to withdraw consent;
    - The right to amend personal data;
    - The right to request that personal data be permanently deleted;
    - The right to strict processing; and
    - The right to raise an official complaint with the relevant authority;

6. Information in relation to any automated processing, for instance profiling, to be carried out, if relevant;

7. Whether personal data must be provided for the purposes of fulfilling or entering into a contract and the outcome should the data subject refuse to provide personal data;

8. Details regarding the destination of the personal data:
    - Whether personal data will be transferred outside of the European Union; and
    - Whether an adequacy decision has been made regarding the destination of the data; and/or
    - Whether any safeguards are in place to ensure the adequacy of the destination; and

9. Any other material that would ensure that the data processing is fair at all times.

All data subjects must be notified prior to the processing of their personal data by Kabuki UK via a FAIR PROCESSING NOTICE, containing the following statements:

For marketing use, whether currently or in the future:

*"Please note that your personal information may be used for marketing purposes n/a. This is not obligatory and you may opt out by emailing: sally@kabukiuk.org.uk, requesting that your personal information be removed. You may also unsubscribe from our electronic marketing content at any time, by selecting the unsubscribe option."*

For marketing use, when specific consent has been provided by the data subject:

*"Please note that you have provided explicit consent for the use of your personal information by Kabuki UK for marketing use n/a. You may withdraw your consent by emailing: sally@kabukiuk.org.uk at any time and you will be immediately withdrawn from all of our marketing lists."*

**4. Responsibilities of DPO**

1. *Consent procedures:* To incorporate procedures in relation to personal data processing based on consent, ensuring that processing ceases when consent is withdrawn;

2. *Consent withdrawal:* To monitor all requests withdrawing consent by keeping a register of all relevant requests and ensuring that all requests are actioned within 24 hours;

3. *Explicit consent:* To ensure that the Fair Processing Notice contains relevant procedures for receiving the relevant consent, when explicit consent is required for marketing purposes due to sectoral requirements or legislation;

4. *Sensitive personal data:* To ensure that the Fair Processing Notice sets out explicitly the purpose or purposes for which sensitive personal data will, or may, be used, when sensitive personal information is collected for a specific purpose or purposes;

5. *Parental consent:* To ensure that parental consent has been provided in relation to all data subjects 16 years of age, or younger;

6. *Data protection law:* To ensure that all new data collection methods comply with data protection laws and good practice, by reviewing and signing off all new such methods;

7. *Fair Processing Notice register:* To maintain an Fair Processing Notice register of all Fair Processing Notices issued, setting out the following information:
    - Fair Processing Notice version number;
    - Issue date and withdrawal date;
    - Location where data will be used;
    - Purpose for which personal data is collected; and
    - Description of expressions, foreign language or formatting, to ensure that the Fair Processing Notice can be fully understood by the target group.

8. *Specified purpose:* To approve all written requests for changes to the purpose of process of personal data and determine if additional consent is required from the data subject:
    - In the event that additional consent is required, to determine the form of the consent and the protocol to be followed by Kabuki UK to ensure that the data subject is informed of the new purpose and has provided the necessary consent;
    - To identify a relevant exemption, when applicable, in the Authorisation to Process; and
    - To update the Data Inventory Schedule 92017-B by setting out details of the new purpose, referring directly to the Authorisation to Process; and

*9.* *Data protection:* To ensure that personal data that is shared with a third party complies with Kabuki UK's notification to the ICO and with the terms of the Fair Processing Notice previously provided to the data subject and any relevant consents provided by the data subject:
    - To ensure that an agreement drafted by Kabuki UK's legal advisors is entered into with the third party, setting out the purpose or purposes for which the information will, or may be, used and listing any restrictions or limitations on the use of the personal information for other purposes;
    - To ensure that the agreement contains an undertaking, or other applicable evidence, by the third party that it is committed to processing its data in such a way that it adheres to the requirements of the DPA at all times;
    - To ensure the agreement contains appropriate controls and safeguards to ensure the protection of personal information pursuant to the GDPR, when such information may be legally shared without the consent of the data subject; and
    - To ensure that any data profiles created by matching data collected by Kabuki UK with other data are not used outside of the context of the ICO notification and the consents of the data subject.

**5. Document owner**

The Data Processor is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated 30.04.2018 is available to all employees of Kabuki UK on the corporate intranet.

This policy document was approved by Kabuki UK's Board of Trustees and is issued by the Chief Executive Officer ("CEO") on a version controlled basis.

Name of CEO: Sally Trewartha Date: 30.04.2018

**Change history record**

| Issue | Description of Change | Approval | Date of Issue |
|---|---|---|---|
| 1 | n/a | n/a | n/a |
| 2 | n/a | n/a | n/a |
| 3 | n/a | n/a | n/a |

# Kabuki UK
# Fair Processing Notice

---

**1. Scope**

This notice applies to all data subjects whose data is processed by Kabuki UK.

**2. Responsibilities**

The Data Protection Officer (“DPO”) is responsible for ensuring that all potential data subjects have sight of this notice prior to the collection and/or processing of their personal data by Kabuki UK.

All employees of Kabuki UK who interact with data subjects are also required to ensure that this notice is brought to the attention of all data subjects, securing their consent for the processing of their personal data.

**3. Fair Processing Notice**

Kabuki UK will use the personal data collected from you for the following purposes:

Family Day Communication, Information Day Communication, Grant Scheme Communication, Local Get Together Information, Newsletter, Fundraising,

You hereby confirm that you are consenting to Kabuki UK’s use of your personal data for the aforementioned purposes(s) and are granting Kabuki UK permission to carry out those actions and/activities.

You may withdraw your consent at any time by reading our Right to Withdraw Consent Procedure 92017-I

**4. What is Personal Data?**

The EU’s General Data Protection Regulation (“GDPR”) defines “personal data” as:

*“any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.*

The GDPR classifies certain data as belonging to “special categories”, as follows:

- Racial origin;
- Ethnic origin;
- Political opinions;
- Religious beliefs;
- Membership to a trade-union;
- Genetic data;
- Biometric data;
- Health data;
- Data concerning a natural person's sex life;
- Sexual orientation; and
- Other.

The GDPR requires that consent is provided by the data subject for all types of personal data, including those pertaining to the special categories set out above and otherwise. Consent must be explicitly provided.

When Kabuki UKrequests sensitive data from data subjects, it is required to confirm why the information is required and how it will be used.

**5. Why does Kabuki UK need to collect and store personal data?**

Kabuki UK is committed to ensuring that all personal information collected and processed is appropriate for the stated purpose(s) and shall not constitute an invasion of your privacy. We may share your personal data with third party service providers who are contracted by us and we shall ensure that they will hold your personal data securely and shall use it only in order to fulfill the service for which they are contracted. When there is no longer a service need, or the contract comes to an end, the third party will dispose of all personal data according to our procedures. We will never share your personal data with third parties until we have received your consent, unless we are required do so by law.

**6. How Kabuki UK uses your information**

Kabuki UK will process your data (i.e. collect, store and use) according to the requirements of the GDPR at all times and shall endeavor to keep your personal data up-to-date, ensuring its accuracy and will not keep it for longer than it is required. In some situations, there are set legal requirements for the length of time that Kabuki UK will retain your personal data but usually Kabuki UK will use its discretion, ensuring that personal data is not kept outside of our usual business requirements.

We shall never be intrusive or invasive of your personal privacy and shall not ask you to provide data that is irrelevant or unnecessary and we will enact strict measures and processes to ensure that the risk of unauthorised access or disclosure of your personal data is minimised as much as possible.

We will only use your personal data for the following purposes:

To give you information about how the charity can help you and what is going on with the charity

**7. Document owner**

The Data Processor is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated {{ insert_date}} is available to all employees of Kabuki UK on the corporate intranet.

This policy document was approved by Kabuki UK's Board of Trustees and is issued by the Chief Executive Officer ("CEO") on a version controlled basis.

Name of CEO: Sally Trewartha Date: 30.04.2018

**Change history record**

| Issue | Description of Change | Approval | Date of Issue |
|---|---|---|---|
| 1 | n/a | n/a | n/a |
| 2 | n/a | n/a | n/a |
| 3 | n/a | n/a | n/a |

# Kabuki UK
# Retention Procedure

## 1. Scope

The retention requirements of this procedure apply to all records held by Kabuki UK, whether in electronic or hardcopy format.

## 2. Responsibilities

Employees in the following roles are responsible for adhering to the following GDPR requirements:

| Role | Responsibility |
|---|---|
| DPO | To ensure that the collection, retention and destruction of all personal data by Kabuki UK is carried out according to the requirements of the GDPR. |
| Finance Director (“CFO”) | To ensure that all financial records, including accounting and tax records are retained. |
| Head of HR | To ensure that all HR records are retained. |
| Health and Safety Officer | To ensure that all Health and Safety records are retained. |
| Company Secretary | To ensure that all relevant statutory and regulatory records are retained (with the exception of the aforementioned records listed above). |
| Change Manager | To ensure that all personal data is stored according to this procedure. |
| Manager/Executive | To ensure that personal data records that are retained are added to business continuity and disaster recovery protocols. |

## 3. Procedure

The DPO is required to maintain a schedule of all personal data items held by Kabuki UK, recording the following information:

- Record name;
- Record type;
- Original owner of personal data;
- Data classification;
- Storage date;

- Retention period required;
- Planned date of destruction; and
- Any additional information such as passwords and cryptographic keys and other means to access the data.

**4. Change Manager**

In relation to storing electronic data, Kabuki UK agrees not to exceed 90% of the manufacturer recommended storage life. The Change Manager shall be responsible for maintaining a schedule of all storage media used by Kabuki UK and their expected shelf life, including the date on which the storage media is due to reach 90% of its expected shelf life.

Once storage media reaches the 90% mark, the Change Manager is responsible for duplicating the data onto a new storage media.

The Change Manager is also responsible for destroying personal data that has reached the end of its retention period and must do so within 30 days. All records that have been destroyed must be listed in a schedule setting out how each type of record was destroyed, by reference to classification and media.

Electronic media stored in portable or removable media must be destroyed according to Disposal of Removable Storage Media 92017-H Policy.

**5. Procedure for accessing stored data**

Kabuki UK shall only access stored data in line with the following procedure:

If anyone were to need access to the members list they would need to request this from the Trustees. The request would only be granted if the activity for which the person requesting the information was directly and only related to the Charities work. If access were to be given it would be with the consent of the Trustees and only in accordance with the rest of our policies. We would never give away or sell personal data and would never use it for anything other than the direct work of the charity.

**6. Document owner**

The Data Processor ( Sally Trewartha) is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated 30.04.2018 is available to all employees of Kabuki UK on the corporate intranet.

This policy document was approved by Kabuki UK’s Board of Trustees and is issued by the Chief Executive Officer (“CEO”) on a version controlled basis.

Name of CEO: Sally Trewartha Date: 30.04.2018

**Change history record**

| Issue | Description of Change | Approval | Date of Issue |
|---|---|---|---|
| 1 | n/a | n/a | n/a |
| 2 | n/a | n/a | n/a |
| 3 | n/a | n/a | n/a |

# Kabuki Uk
# Privacy Impact Assessment

---

## 1. Scope

Kabuki Uk's data processing activities will undergo an initial Privacy Impact Assessment ("PIA") and subsequent PIAs throughout its lifecycle.

A subsequent PIA may be carried out in the following circumstances:

- When setting up a new IT system;
- When new legislation, policies or related matters affecting privacy, are developed;
- When launching a data sharing initiative; and/or
- When personal data is used for new purposes.

## 2. Responsibilities

The Data Protection Officer ("DPO") is responsible for determining whether a full PIA is required. He or she shall reach this decision based on a PIA questionnaire, which must be undertaken for the purposes of making such a determination.

All completed PIAs will be signed off by the Board of Trustees.

## 3. Process

The DPO shall at all times conduct PIAs by direct reference to the Information Commissioner's Office ("ICO") Code of Practice.

The DPO may seek specialist advice regarding privacy, should he or she feel it is required.

The DPO shall record all outcomes, including whether or not a PIA is required, in the ICO Code of Practice Annexes.

The DPO shall record in all change control processes that a PIA has been considered.

## 4. Document owner

The Sally Trewartha is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated 28.04.2018 is available to all employees of Kabuki Uk on the corporate intranet.

This policy document was approved by Kabuki Uk's Board of Trustees and is issued by the Chief Executive Officer ("CEO") on a version controlled basis.

Name of CEO: Sally Trewartha Date: 28.04.2018

**Change history record**

| Issue | Description of Change | Approval | Date of Issue |
|---|---|---|---|
| 1 | n/a | n/a | n/a |
| 2 | n/a | n/a | n/a |
| 3 | n/a | n/a | n/a |

# Kabuki UK
# Third Party Access to Data

---

## 1. Scope

Kabuki UK is responsible for ensuring the security of its data processing facilities and other information assets in relation to third parties. This procedure applies to all situations where third parties require access to any of Kabuki UK's data, including all of the following categories of external parties with whom Kabuki UK may have agreements in place:

- Service providers, including managed security service providers;
- Clients and customers;
- Outsourcing suppliers including: facilities, operations, IT systems, data collection and call centers;
- Consultants;
- Auditors;
- Providers of IT systems and services;
- Providers of cleaning, catering and other outsourced support services; and
- Temporary staff, including placement and other short-term appointments.

Kabuki UK is responsible for assessing associated third-party risks according to the category and level of risk involved.

## 2. Responsibilities

Where there is a business requirement to work with third parties, Kabuki UK is required to enter into a formal agreement regarding information security with all third-party service providers.

The Data Protection Officer ("DPO") and all third-party relationship owners responsible for the aforementioned service categories are required to ensure that formal external party contracts are entered into in line with this procedure. All contracts must implement adequate security controls, delivery levels and service definitions and the DPO and third-party relationship owners are responsible for ensuring that these are properly implemented and maintained by the third party, carrying out risk assessments as and when required by this procedure.

Throughout any transition periods Kabuki UK shall offer the same level of security.

## 3. Procedure

Kabuki UK shall only grant third parties access to organisational assets, including personal data and other information, once a risk assessment has been carried out and the appropriate systems and controls are implemented.

*Risk assessment - step by step*

1. Kabuki UK carries out a risk assessment and identifies all risks pursuant to third party access to data.

2. For each third party, the risk assessment shall identify the following:

    - The data and the processing facilities which the third party will have access to;
    - The type of access the third party shall have, whether physical and/or logical, whether on or off-site;
    - The exact location from which the third party will access the data;
    - The value and specific classification of the information which the third party will access;
    - The data to which the third party shall not be granted access and which may need to be secured by additional means;
    - A full list of the third party's personnel who will be or are likely to be involved in the access to data, including partners and external contractors;
    - How the third party's personnel shall be authenticated;
    - How the third party intends to store, process and communicate the data;
    - The impact that inaccurate, incorrect or misleading data shared with the third party would have on the third party;
    - The impact on the third party of a potential inability to access the data when required;
    - How Kabuki UK's Security Incident Management Procedure applies and should be implemented if and when information security incidents take place, which involve the third party;
    - Any legal or regulatory matters regarding the third party that are of note; and
    - How Kabuki UK's stakeholder interests may be affected by any of the decisions made in relation to the third party relationship.

3. All systems and controls implemented by Kabuki UK pursuant to the risk assessment must be according to the GDPR and must be within the power of Kabuki UK.

4. Kabuki UK and the third party agree to implement appropriate controls and Kabuki UK's legal advisors shall draw up a contract, which the third party is required to sign. Amongst the third party's obligations is the requirement that all of its personnel are aware of their obligations pursuant to the contract.

5. When drafting the contract, Kabuki UK's legal advisers are required to consider and include all of the following information security policy matters and insofar as any matters are not included within the contract, must provide a documented reason why they was not included, as well as the requirement under which they were identified as part of the risk assessment:

- A clear definition and/or description of the service or product provided by the third party and a description of the data and its classification;
- Training, education and awareness requirements for all third party users;
- Any provisions for the transfer of personnel;
- Responsibilities for the installation of software and hardware, as well as maintenance and destruction;
- A robust and clearly defined process of reporting, including structural requirements, reporting formats and escalation protocols;
- A requirement that the third party adequately resources reporting, monitoring and compliance activities;
- A robust and clearly defined change management process;
- An Access Control Policy, refer to Security Access Policy 92017-G;
- Physical controls, including secure areas;
- Controls against malware;
- Data security incident management;
- Appropriate service and security levels, including what would amount to unacceptable service and security, as well as a clearly defined verifiable criteria of performance and security, monitoring and reporting;
- The right for Kabuki UK to monitor and audit the performance of the third party, for which Kabuki UK may use external auditors, including the third party's processes for change management, identifying vulnerabilities and managing information security incidents, as well as Kabuki UK's right to revoke activities;
- The requirements of service continuity;
- Legal responsibilities and liabilities and how they shall be met;
- Copyright and Intellectual Property Rights protection;
- Systems and controls in relation to subcontractors; and
- Conditions for renegotiation and termination of agreements and contingency plans.

**4. Information transfer agreements**

When the contract between Kabuki UK and a third party is for the transfer of data or software, the following additional controls must be considered, pursuant to an individual risk assessment:

- How the management of both Kabuki UK and of the third party shall be responsible for notifying transmission, dispatch and receipt of data as well as any associated procedures and controls;
- Systems and procedures for ensuring the traceability and non-repudiation of data;
- The means of data transmission;
- Packaging of data;
- Agreed system of labelling the data;
- The selection of couriers and methods of identification;
- The management of data security incidents;

- Escrow agreements;
- Copyright, data protection and software licensing;
- Technical requirements for recording or reading data or software; and
- Any other systems and controls such the use of cryptography.

**5. Managing changes to third party services**

Please also refer to Security Access Policy 92017-G

Kabuki UK may need to agree to variations to contracts with third parties, as a result of the following potential changes:

- The service it currently offers;
- The implementation of new systems or applications;
- Updates or modifications to its policies and procedures; and
- Updated systems and controls arising from new risk assessments or data security incidents.

A third party may require changes to its contract with Kabuki UK as a result of the following potential changes:

- New networks and infrastructure;
- New technologies, products or new releases of current products;
- New physical locations;
- New physical services;
- New tools or methodologies;
- New service providers; and
- New suppliers of hardware or software.

If any changes arise, a new risk assessment and review of the selected controls must be carried out. Any changes to the contract based on the introduction of new controls, or the amendment of existing controls must be agreed with the third party and inserted into the contract via an agreed variation.

The DPO and relationship owners are responsible for ensuring that the new controls are implemented and incorporated into review and monitoring arrangements already in place.

**6. Document owner**

The Data Processor is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated 30.04.2018 is available to all employees of Kabuki UK on the corporate intranet.

This policy document was approved by Kabuki UK's Board of Trustees and is issued by the Chief Executive Officer ("CEO") on a version controlled basis.

Name of CEO: Sally Trewartha Date: 30.04.2018

**Change history record**

| Issue | Description of Change | Approval | Date of Issue |
|---|---|---|---|
| 1 | n/a | n/a | n/a |
| 2 | n/a | n/a | n/a |
| 3 | n/a | n/a | n/a |

# Kabuki UK
# Data Processing by External Suppliers

## 1. Scope

This procedure covers all situations where external suppliers are used by Kabuki UK to process personal data on its behalf.

## 2. Responsibilities

It is the responsibility of the Data Protection Officer (“DPO”) to approve all subcontractors used by Kabuki UK to process personal data on its behalf, according to the requirements of this procedure.

It is the responsibility of the owners of third-party relationships to ensure that all data processing by third parties is carried out according to the requirements of this procedure.

The third party relationship owner shall be assisted by the Head of IT, who shall be responsible for providing technical and other assistance and resources to provide assistance.

Regular audits of third-party compliance shall be carried out by the Quality Manager, who shall be responsible for them.

## 3. Procedure

Kabuki UK shall only engage with third party data processors that are able to provide security, including technical, physical or organisational security, to all personal data that they process on Kabuki UK’s behalf.

In addition to other circumstances set out elsewhere in this procedure, Kabuki UK shall only engage with third party processors outside of the EU in the following circumstances:

- When the third-party data processor has been identified positively in an EU Commission adequacy decision; or
- When the rights and freedoms of data subject are secured by legally binding corporate rules and other safeguards, agreed between Kabuki UK and the third-party data processor and are equal or equivalent to those afforded by the EU; or
- Where a specific arrangement between Kabuki UK and the third-party data processor has been approved by the Information Commissioner or the supervisory authority.

Before entering into any agreement with a third-party data processor, Kabuki UK must carry out an information security risk assessment.

Taking into consideration the basis of the nature of the personal data to be processed and the specific circumstances of the data processing, the DPO may deem it necessary that an additional audit of the third-party data processor's security arrangements may be carried out before entering into any agreement.

Kabuki UK shall only engage a third-party processor pursuant to a written contract which expressly sets out the service to be provided. The third-party processor is also required to provide suitable security for the personal data to be processed, which must also be confirmed in the written contract ("the data processing contract").

Kabuki UKis required to carry out regular audits of the third-party data processor's security arrangements throughout the duration of the contract, when the third party has access to personal data held by Kabuki UK.

The data processing contract must contain a clause preventing third-party data processors from hiring subcontractors for the processing of personal data in the absence of express, written approval by Kabuki UK.

Kabuki UK will only approve contracts with second-tier data processors, if the subcontractors of the third-party data processor agree to provide the same level of security and protection to the rights and freedoms of the data subject as those afforded by Kabuki UK. In addition, the contract between the third-party data processor and the second-tier data processors must contain a clause requiring that all personal data will be either destroyed or returned to Kabuki UK upon the termination of the contract.

**4. Document owner**

The Data Controller is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated 30.04.2018 is available to all employees of Kabuki UK on the corporate intranet.

This policy document was approved by Kabuki UK's Board of Trustees and is issued by the Chief Executive Officer ("CEO") on a version controlled basis.

Name of CEO: Sally Trewartha Date: 30.04.2018

**Change history record**

| Issue | Description of Change | Approval | Date of Issue |
|---|---|---|---|
| 1 | n/a | n/a | n/a |
| 2 | n/a | n/a | n/a |
| 3 | n/a | n/a | n/a |

# Kabuki UK
# Data Protection Officer Policy

---

**1. Main Purpose**

To ensure compliance with the EU General Data Protection Regulation ("GDPR") and provide for ongoing compliance of all Kabuki UK's activities.

**2. Position**

The Data Protection Officer ("DPO") reports directly to Kabuki UK's Board of Trustees and is a member of the Information Security Committee.

The current Data Protection Officer is Sally Trewartha.

**3. Responsibilities**

The DPO is an expert in data protection law and practice and shall advise on and ensure that Kabuki UK is compliant with the requirements of the GDPR, based on Kabuki UK Board of Trustees agreeing to and implementing all Policy Documents and Procedures relating to the GDPR at all times, as well as other relevant UK data protection law and regulation.

It is the responsibility of the DPO to ensure that all of Kabuki UK's policies and procedures are maintained and kept up to date and that data processing audits are regularly carried out to ensure that Kabuki UK's core activities comply with the GDPR.

The Employees of Kabuki UK shall liaise with Kabuki UK's appointed DPO on all data protection matters.

Pursuant to Article 39, 1,a-e GDPR, the main tasks of the DPO are as follows:

1. To provide information and advice to Kabuki UK, including its partners, suppliers and contractors on all matters of data protection and compliance with the GDPR and UK law;

2. To liaise with and advise all employees of Kabuki UK regarding their obligations under the GDPR and UK law in relation to personal data;

3. To monitor compliance with the GDPR and UK law by carrying out audits of processes pertaining to personal data, reporting the findings to the Board of Trustees and to allocate internal responsibilities to ensure ongoing compliance;

4. To help develop and maintain Kabuki UK's Data Protection policies, processes and procedures in relation to personal data;

5. To facilitate the delivery of training for all employees of Kabuki UK, who are involved in processing personal data;

6. To advise on data protection impact assessments and performance monitoring, as per the requirements of the GDPR;

7. To liaise with the supervisory authority and to be the main point of contact on all issues pertaining to personal data, consulting with the supervisory authority when necessary;

8. To advise on effective security procedures and monitor compliance;

9. To advise on and help develop incident reporting procedures and investigations;

10. To advise on information security processes and allocation of responsibility;

11. To assist with the development of business continuity planning;

12. To advise on the processes for monitoring the copying of proprietary software;

13. To advise on the safeguarding of organisational records; and

14. To advise on personal data that is collected by Kabuki UK, is properly controlled and safeguarded.

The DPO shall have access at all times to Kabuki UK's personal data collection, processing and storage systems. All Kabuki UK, employees are required to assist the DPO in engaging in these duties, including providing access to records and systems if requested. Failure by Kabuki UK, employees to assist the DPO accordingly, will be reported to the Board of Trustees .

**4. Document owner**

The DPO is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated 30.04.2018 is available to all employees of Kabuki UK on the corporate intranet.

This policy document was approved by Kabuki UK's Board of Trustees and is issued by the Chief Executive Officer ("CEO") on a version controlled basis.

Name of CEO: Sally Trewartha Date: 30.04.2018

**Change history record**

| Issue | Description of Change | Approval | Date of Issue |
|---|---|---|---|
| 1 | n/a | n/a | n/a |
| 2 | n/a | n/a | n/a |

| | | | |
|---|---|---|---|
| 3 | n/a | n/a | n/a |

# Kabuki UK
# Personal Data Transfer Outside of the EU

## 1. Scope

Kabuki UK is required to follow this procedure when it intends to engage in the transfer of personal data to countries or to international organisations outside of the EU for processing, as per the requirements of the GDPR, including the transfer of personal data from a country or an international organisation to another country or another international organisation.

## 2. Responsibilities

Kabuki UK must ensure that all of the personal data of natural persons in its control is suitably protected, in line with the GDPR.

## 3. Transfer procedure

Kabuki UK, as data controller or data processor, shall ensure that adequate protection is provided to the data subject whose personal data is being transferred to countries or to international organisations outside of the EU by ensuring the following:

1. That it has checked the *Official Journal of the European Union* and confirmed that the country of the recipient of the personal data is an approved country, as per the EU list of approved countries. This also applies to industry sectors within particular countries;

2. That the country of the recipient of the personal data has adequate data protection systems and controls, whether by statute or self-regulation;

3. That it has an agreement in place which the recipient of the personal data, incorporating existing and/or approved data protection clauses, ensuring the data subject is adequately protected;

4. That it is transferring the personal data pursuant to approved binding corporate rules;

5. That it is applying one of the exemptions set out at clause 10 of the GDPR Data Protection Policy 92017-A, namely that:

    a. Explicit consent has been provided by a fully informed data subject, who has been made aware of all possible risks involved in light of appropriate safeguards and an adequacy decision;
    b. The personal data transfer is a prerequisite to the performance of a pre-existing contract between the data controller and the data subject or when the data subject requests that pre-contractual measures are implemented;

c. The personal data transfer is a prerequisite to the conclusion or performance of a pre-existing contract between the data controller and another person, whether natural or legal, if it is in the interest of the data subject;

d. The personal data transfer is in the public interest;

e. The personal data transfer is required for the creation, exercise or defence of legal claims;

f. The data subject is not capable of giving consent, whether due to physical or legal limitations or restrictions and the personal data transfer is necessary for the protection of the key interests of the data subject or of other persons, whether natural legal; and

g. The personal data transfer is made from an approved register, confirmed by EU or Member State law as having the intention of providing public information and which is open to consultation by the public or by an individual demonstrating a legitimate interest, but only so far as the legal requirements for consultation are fulfilled; and

6. That it is relying on approved certification mechanisms or codes of conduct alongside binding agreements in the country or international organisation outside of the EU that set out appropriate safeguards for the protection of the rights of personal data subjects.

**4. Document owner**

The Data Processor is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated 30.04.2018 is available to all employees of Kabuki UK on the corporate intranet.

This policy document was approved by Kabuki UK's Board of Trustees and is issued by the Chief Executive Officer ("CEO") on a version controlled basis.

Name of CEO: Sally Trewartha Date: 30.04.2018

**Change history record**

| Issue | Description of Change | Approval | Date of Issue |
|---|---|---|---|
| 1 | n/a | n/a | {{ insert_date_1 }} |
| 2 | n/a | n/a | n/a |
| 3 | n/a | n/a | n/a |

# Kabuki UK
# Right to Withdraw Consent Procedure

## 1. Scope

This procedure covers all situations where, as per the GDPR, the data subject wishes to withdraw his or her consent for personal data processing.

Withdrawal of consent is defined as any indication on the part of the data subject that he or she withdraws consent for the processing of their personal data. Withdrawal of consent must be specific and without ambiguity and shall be provided by the data subject either by way of a statement or through clear, affirmative action on his or her part.

Withdrawal of consent by the data subject covers all processing activities carried out for a specific purpose or purposes, for which that data subject provided consent in the first place.

Withdrawal of consent shall not make unlawful any processing of personal data engaged in by Kabuki UK prior to the withdrawal of consent.

## 2. Responsibilities

As a data controller, Kabuki UK is responsible for administering the withdrawal of consent on the part of the data subject, under the oversight of the Data Protection Officer (“DPO”).

## 3. Withdrawal of consent procedure

Withdrawal of consent is indicated via the Data Subject Withdrawal of Consent Form 92017-J and Kabuki UK must be able to demonstrate that the data subject has withdrawn consent, by producing the completed form, if required.

If Kabuki UK was processing the data for multiple purposes, Kabuki UK must be able to show that consent has been withdrawn for all purposes.

## 4. Withdrawal of parental consent procedure

Withdrawal of consent by a holder of parental responsibility is indicated via the Withdrawal of Parent Consent Form 92017-K and Kabuki UK must be able to demonstrate that the data subject has withdrawn consent, by producing the completed form, if required.

Kabuki UK must be able to demonstrate that it has taken reasonable efforts to ensure that the claim of parental responsibility is authentic and true, when consent is withdrawn for a child data subject, including the use of available technology.

**5. Document owner**

The Data Processor is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated 30.04.2018 is available to all employees of Kabuki UK on the corporate intranet.

This policy document was approved by Kabuki UK's Board of Trustees and is issued by the Chief Executive Officer ("CEO") on a version controlled basis.

Name of CEO: Sally Trewartha Date: 30.04.2018

**Change history record**

| Issue | Description of Change | Approval | Date of Issue |
|---|---|---|---|
| 1 | n/a | n/a | {{ insert_date_1 }} |
| 2 | n/a | n/a | n/a |
| 3 | n/a | n/a | n/a |

# Kabuki UK
# Data Subject Consent

## 1. Scope

This procedure covers all situations where Kabuki UK requires the consent of a data subject for the processing of personal data.

Consent is defined as any indication on the part of the data subject that he or she agrees that their personal data may be processed. Consent must be given freely, without any duress, it must be specific, informed and without ambiguity and shall be granted by the data subject either by way of a statement or through clear, affirmative action on his or her part.

## 2. Responsibilities

As a data controller, Kabuki UK is responsible for obtaining the consent of the data subject, under the oversight of the Data Protection Officer ("DPO").

## 3. Consent procedure

Kabuki UK must demonstrate that explicit consent has been given for the processing of a data subject's personal data. This is done via a Data Subject Consent Form 92017-N.

The specific purpose or purposes of the processing must be set out in the Data Subject Consent Form and the data subject must expressly consent to this.

Kabuki UK must be able to demonstrate the following:

- That the consent of the data subject is easily distinguishable from all other data held on the data subject (i.e. it is easy to locate and identify);
- That the consent of the data subject is made in an intelligible manner, using clear and plain language;
- That, prior to giving consent, the data subject has been informed of his or her rights to withdraw consent, as per the Right to Withdraw Consent Procedure 92017-I; and
- That the processing of personal data can only take place pursuant to the agreement between Kabuki UK and the data subject, whereby the data subject provides his or her explicit consent.

**4. Child consent procedure**

In relation to the processing of personal data of children under the age of 16, Kabuki UK requires additional consent from the person who has parental responsibility over the child and Kabuki UK must be able to demonstrate that this additional consent has been provided, as per Parental Consent Form 92017-L and that it has taken reasonable efforts to ensure that the claim of parental responsibility is authentic and true, including the use of available technology.

**5. Document owner**

The Data Processor is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated 30.04.2018 is available to all employees of Kabuki UK on the corporate intranet.

This policy document was approved by Kabuki UK's Board of Trustees and is issued by the Chief Executive Officer ("CEO") on a version controlled basis.

Name of CEO: Sally Trewartha Date: 30.04.2018

**Change history record**

| Issue | Description of Change | Approval | Date of Issue |
|---|---|---|---|
| 1 | n/a | n/a | n/a |
| 2 | n/a | n/a | n/a |
| 3 | n/a | n/a | n/a |

# Kabuki UK
# Personal Data Breach

---

## 1. Scope

This procedure applies in the following events:

1. A personal data breach pursuant to Article 33 '*Notification of a personal data breach to the supervisory authority',* and

2. A personal data breach pursuant to Article 34 *'Communication of a personal data breach to the data subject'* of the GDPR.

## 2. Data controller and data processor

There is a distinction under the GDPR between a 'data controller' and a 'data processor'. This is because different organisations involved in processing personal data have varying degrees of responsibility. An organisation must choose whether it is a data controller or a data processor as regards a particular activity and cannot be both.

## 3. Responsibility

All users, including temporary employees of Kabuki UK and third parties, and Kabuki UK must be aware of this procedure and are required to follow it should a personal data breach incident occur.

## 4. Procedure – Breach Notification

*Data processor to data controller*

All personal data breaches by Kabuki UK must be notified to the appropriate data controller immediately. The Data Protection Officer ("DPO") must record the communication of the breach in the Internal Personal Data Breach Register 92017-Y, stating how the notification was made (whether my email, telephone call etc.), to whom and how the confirmation of receipt was provided.

*Data controller to supervisory authority*

All personal data breaches by Kabuki UK must be notified to the appropriate supervisory authority immediately.

Kabuki UK is required to carry out an assessment in order to determine whether the personal data breach is likely cause a risk to the affected data subject's rights and freedoms under the GDPR.

If a risk is considered likely, Kabuki UK is required to report the personal data breach to the supervisory authority immediately and in any event, no later than 72 hours after the risk assessment. If the notification is made outside of the 72 hour window, Kabuki UK is required to provide reasons for the delay.

Pursuant to External Breach Notification Record 102017-A1, Kabuki UK is required to provide the following to the supervisory authority:

- A description of the nature of the personal data breach;
- The categories of personal data that have been affected by the breach;
- The number, which may be approximated if necessary, of data subjects affected by the breach;
- The number, which may be approximated if necessary, of personal data records affected by the breach;
- The name and contact details of the DPO;
- The likely outcomes of the personal data breach;
- Any measures taken by Kabuki UK to address and/or mitigate the breach; and
- All other information regarding the data breach.

The DPO must record the communication of the breach in the Internal Personal Data Breach Register 92017-Y, stating how the notification was made (whether my email, telephone call etc.), to whom and how the confirmation of receipt was provided.

*Data controller to data subject*

If it is likely that there will be a high risk to the affected data subject's rights and freedoms under the GDPR, Kabuki UK is required to provide immediate notification to the relevant data subjects.

The notification to the data subject must be made in clear and plain language and must include the following:

- A description of the nature of the personal data breach;
- The categories of personal data that have been affected by the breach;
- The number, which may be approximated if necessary, of data subjects affected by the breach;
- The number, which may be approximated if necessary, of personal data records affected by the breach;
- The name and contact details of the DPO;
- The likely outcomes of the personal data breach;
- Any measures taken by Kabuki UK to address and/or mitigate the breach; and
- All other information regarding the data breach.

Kabuki UK must use appropriate measures, such as encryption, to ensure that all personal data is secure and cannot be accessed by those without the requisite authority.

Kabuki UK must also take subsequent measures to ensure that the risk to the rights and freedoms of the data subject are no longer an issue.

If notification would require Kabuki UK to implement a disproportionate amount of effort, a public communication or other similar measure may suffice, so long as all data subject are effectively informed.

It is possible that the supervisory authority may require Kabuki UK to communicate the personal data breach to the data subject, should there be an element of high risk involved.

**5. Document owner**

The Data Processor is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

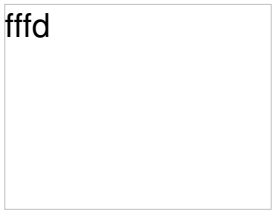
The latest version of this policy document dated 30.04.2018 is available to all employees of Kabuki UK on the corporate intranet.

This policy document was approved by Kabuki UK's Board of Trustees and is issued by the Chief Executive Officer ("CEO") on a version controlled basis.

Name of CEO: Sally Trewartha Date: 30.04.2018

**Change history record**

| Issue | Description of Change | Approval | Date of Issue |
|---|---|---|---|
| 1 | n/a | n/a | n/a |
| 2 | n/a | n/a | n/a |
| 3 | n/a | n/a | n/a |


fffd