CSM AUSTRALIA - INTERNAL POLICIES

These policies apply to all CSM staff. Please select a link below to read the relevant policy:

1. Working with Children
2. Employee Code of Conduct
3. Employee Social Media Policy
4. Employment of Ex-Offenders Policy
5. Whistleblowing Policy
6. Employee Data Protection Policy
7. Data Protection Fact Sheet
8. Criminal Records Check Policy
9. Questions

1. OUTLINE FOR WORKING WITH/MARKETING TO CHILDREN AND VULNERABLE ADULTS

In the UK there is specific legislation for those working with children and vulnerable adults (as defined below). Legislation varies in our different group countries but being a UK registered company we need to ensure that our activities are compliant with UK requirements, wherever we work.

This document applies in Australia and is adapted from the equivalent UK/Global document.

Set out below is a checklist to be followed if CSM engages CSM staff, contractors or volunteers to work with such groups of people, directly or on behalf of clients.

"Working With" Children

In the UK, "child" means anyone up to the age of 18.

In Australian States and Territories, "**child**" means a person under the age of 18 years.

What Activity is covered?

In Australia, the activities covered differ between each State/Territory. Please see the summary table attached.

In the UK, the following activities are covered:

- Regularly training and instructing (eg. long-term internships, or training for a performance or volunteering);
- Regularly providing guidance on well-being;
- Regularly driving a children-only vehicle;
- Supervising anyone doing the above; and
- Anyone working in a school, children's home, or childcare premises.

NOTE: One-time short-term work experience or internships for children are NOT covered but if an employee or contractor regularly manages short-term work experience or internship programmes, s/he will be subject to the legislation.

"Working With" Vulnerable Adults

In the UK, "vulnerable adult" means anyone in receipt of any of the activities listed below.

What Activity is Covered?

- Providing any health care or personal care;
- Transporting between residences or care facilities (for example, transporting ill, aged or disabled adults); and
- Supervising anyone doing the above.

In Australia, only the ACT has a statutory scheme in relation to "**vulnerable adults**". Please see the summary table attached.

Checklist to be Followed

- CSM has developed and published internally a policy for safeguarding children and vulnerable adults covering:

  a. Identification of relevant situations within CSM and for clients;

  b. Reporting any concerns about treatment; and

  c. Appointing a member of staff as the Safeguarding Officer (in the UK, the CSM Safeguarding Officer is Michelle Comerton, CSM's Group People and Talent Manager; in Australia, the CSM Regional Safeguarding Officer is Rob Smith, Managing Director, CSM).

  This policy can be found at [URL]. Please ensure that you have read it.

- The relevant Account Director must identify which staff, contractors and volunteers will be working with children and/or vulnerable adults as defined above in activities as specified above and must inform the Safeguarding Officer.
- Each such person (staff, contractor and volunteer) must complete CSM's children and vulnerable adults' education and training programme.
- The Account Director must check with CSM's Group Legal Counsel with respect to the insurance provisions of the relevant activity/client work.
- The Safeguarding Officer will ensure that for each person carrying out activity which falls under the legislation (outlined in the attached table) has a Working With Children Check (or equivalent).
- CSM's Group Legal Counsel will advise what other legislation may apply. A brief summary of the type of activity, the people involved, the location and timing must be provided to CSM's Group Legal Counsel at least 10 days in advance of the activity commencing and prior to the recruitment of employees, contractors or volunteers.

Commercial Use of Pictures or Other Images of Children

The following general principles apply and must be followed by the Account Director:

- If the child is reasonably identifiable, Australian privacy laws apply (see below);
- Ensure that any image and its use are appropriate (refer, for example, to the Australian Association of National Advertisers *Guideline for Managing Images of Children & Young People*); or
- If the child is not reasonably identifiable, but his or her face is clearly visible, it is CSM policy to seek and record written consent for use from the child's parent or guardian.

Direct Marketing/Obtaining Any Personal Information From Children

- Personal information means information or opinion about an identified individual – this includes any pictures identifying children by name, or contact details provided in response to a commercial promotion or advertising campaign.
- Consent of the children's parent or guardian must be obtained prior to collecting personal information.
- A copy of CSM's privacy collection statement should be provided at the time consent is obtained.
- The Account Director must check and approve the contents of any marketing or promotional communication aimed at children. It is CSM policy that such material must not contain anything which:
  - is likely to result in physical, mental or moral harm; or
  - exploits credulity, loyalty, vulnerability or lack of experience.

Advertising/marketing material aimed at children should be reviewed for compliance with applicable codes including the Australian Association of National Advertisers *Guideline for Managing Images of Children & Young People* and, where applicable, the ACMA *Children's Television Standards* and the *Commercial Television Industry Code of Practice*.

If there is any doubt regarding content, please check with CSM's Group Legal Counsel.

2. EMPLOYEE CODE OF CONDUCT

The Chime Group aims to conduct its business with honesty and in good faith, free from fraud and deception.

In order to achieve this, all Chime Group employees must follow our **Codes of Conduct**:

- We will respect client and company confidentiality.
- We will encourage a meritocracy, promoting employees on the basis of their qualifications and merit, without discrimination or concern for race, national origin, colour, sex, sexual orientation, age or disability.
- The people of Chime expect the Group to be a civilised and safe place to work. We will respect each other and not engage in, or condone, sexual or racial harassment and discrimination, or offensive behaviour of any kind.
- We do not knowingly create or distribute work which contains statements or images offensive to general public decency.
- We will not use, possess or distribute illegal drugs.
- We will maintain honest business practice – we do not, for example, offer or solicit bribes or inducements.
- We will comply with all laws and regulations, national or international, that could be construed as connected with our business.

3. SOCIAL MEDIA POLICY

Overview

For the purpose of this policy, Social Media refers to those tools and channels online and with mobile devices that allow people to share views, images, links and other content. They include Facebook, Twitter, Flickr, LinkedIn, Vine, Snapchat, Pinterest etc.

The Challenge of Social Media

Social Media has an increasing part to play in business, and much of our work involves us in using Social Media for our clients and as part of our public profile. Social Media, when used well, can enhance reputation and enhance the impact of campaigns. When used badly, it can damage or destroy reputations rapidly.

Attitudes to Social Media in business vary widely, including:

- Laissez-faire – a belief that Social Media is like a human right and only requires the lightest touch monitoring of usage;
- Disinterest – no real awareness or interest in the uses and abuses of social media;
- Police state – a belief that Social Media is unnecessary and that its use should be minimised.

We have taken these challenges into account in setting out this policy.

All official use of Social Media on behalf of CSM and to promote CSM business will be managed in the same way all our official communications are managed, with sign-off through MDs and adherence to CSM content and style guidelines. Whether, and how, you use Social Media for your own personal communications is a matter for you to decide. However, in doing so you should be mindful of the potential impact of Social Media, and we ask that you follow these guidelines

Guidance on Social Media

Think before you post

- Alcohol and Social Media do not generally play well together.
- If you're unsure, you probably shouldn't post it.
- Your posts are a broadcast to the world. Assume that everyone can see them.
- Even if you delete a post, it will have been seen and possibly re-posted already.
- Even if you tweet anonymously or under a pseudonym, you can be traced.

Be Respectful

- If you wouldn't say something to someone's face, don't say it to them online.
- Nuances are hard to detect. What you see as banter might be seen as intimidating.
- Try to add constructively to the conversation. Opinions/Debates are healthy; Rudeness/Personal attacks are not.
- It's worth checking someone's bio before getting into an online debate with them – they may be a spammer or angling for a rise from you.

Tips and Tricks

- When asking people to share a client's tweet, ask them to re-tweet the original tweet, rather than tweet a copy.
- Setting your social media accounts to private is no 'real' guarantee of privacy.
- You are as accountable for your actions via Social Media as you are in any other form of communication.
- Followers/Fans are not the be all and end all of social media. Engagement with your audience is a more reliable path to positive outcomes.
- If you start a tweet with @name only you, @name and your mutual followers can see it. This is also what happens automatically when you hit 'reply' to a tweet. Note: This doesn't make the conversation private and it will still be visible on your profile page.

Contractual Obligations

- The confidentially clauses within your employment contract DO apply with social media. Be mindful of both sensitive client and company information.
- Misuse of Social Media may constitute gross misconduct under your employment contract.
- A breach of your contractual obligations, including those policies outlined in the CSM Australia handbook will be treated the same regardless of the medium. Social Media is not an exception to this rule!

4. EMPLOYMENT OF EX-OFFENDERS - POLICY

Introduction

CSM is committed to the equal treatment of all employees and applicants and requires all employees, at all levels, to abide by this general principle. The aim of this policy is to state CSM's approach towards employing people who have criminal convictions.

CSM promotes equality of opportunity for all job applicants and aims to select people for interview and for employment based on their individual skills, abilities, knowledge, experience and, where appropriate, qualifications, training and potential.

CSM, therefore, will consider ex-offenders for employment. Within the UK, however, our approach differs depending on whether the job is or is not exempt from the provisions of the UK Rehabilitation of Offenders Act 1974 (**Act**).

This policy statement should be read in conjunction with CSM's policy on Equal Opportunities and its policy on the use of disclosure information.

Audience: All staff. This policy may be copied to third parties to evidence our policy.

Jobs Covered By The Rehabilitation Of Offenders Act 1974:

Most UK-based jobs within CSM are covered by the Act and, therefore, job applicants will only be asked to disclose any **unspent** convictions.

When the job offer is made (or in some cases during the selection and interview process), CSM will ask job applicants to complete a Criminal Record Declaration Form (**Form**). For roles which are not exempt from the Act, this form does not ask questions about any spent convictions and applicants are not expected to disclose any spent convictions. Applicants are made aware that the information they provide may be checked and that giving false information or deliberately omitting information may disqualify them for employment. The Form is returned to a designated person within CSM with the option to provide details in a confidential envelope and we guarantee that this information will only be seen by those who need to see it as part of the recruitment process.

In order to check the information provided the job applicant may be required to apply for a Basic Disclosure via Disclosure Scotland. CSM will meet the cost of the check.

CSM will not automatically refuse to employ someone who has a previous criminal conviction if the offence is not relevant to the role and does not make the applicant a risk in the role for which they have applied. If the nature of the offence is relevant to the job, CSM will review the circumstances and may, at its discretion, decline to select the applicant or, if an offer has already been made, following discussion with the applicant, CSM may withdraw the offer.

Jobs That Are Exempt from The Act

In order to protect certain vulnerable groups within society, within the UK some posts and professions are exempted from the Act, including, but not limited to, posts involving access to children, young people, the elderly and disabled and financial management. Some UK-based jobs within CSM are exempted from the Act and, if CSM is seeking to recruit someone into such a job, an applicant will be required to disclose all convictions about which CSM is legally allowed to know, which may include spent as well as unspent convictions.

When a job offer is made (or in some cases during the selection and interview process), CSM asks all job applicants to complete a Form. For roles which are exempt from the Act, this form asks about all convictions, whether spent or unspent, which are not "protected" as defined by the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (as amended in 2013). The Form is returned to a designated person within CSM with the option to provide details in a confidential envelope and we guarantee that this information will only be seen by those who need to see it as part of the recruitment process.

Subsequently CSM will seek documentary evidence about the person's criminal convictions. This is done through a joint application to the Disclosure & Barring Service (**DBS**) for a Standard, Enhanced or Enhanced with DBS Barred Lists check (as appropriate to the role in question). CSM will pay for the DBS check.

The appropriate DBS check is only requested after a thorough risk assessment has indicated that one is both proportionate and relevant to the position concerned. Applicants for exempt roles are made aware that an application for a DBS certificate will be required and offers are made subject to the outcome of such checks. We encourage all applicants called to an interview for exempt roles to provide details of any criminal record at an early stage in the application process.

Further Information

Where it is necessary to decide whether or not a suitable applicant who has a criminal record should be appointed or not, the decision is only made by an appropriate HR or Security authority who has been suitably trained to identify and assess the relevance and circumstances of offences and who has received appropriate guidance and training in the relevant legislation relating to the employment of ex-offenders (e.g. the Act).

At interview, or in a separate discussion with an applicant, we ensure that an open and measured discussion takes place on the subject of any offences or other matter that might be relevant to the position. We undertake to discuss any matter revealed in a Disclosure with the person seeking the position before withdrawing a conditional offer of employment.

We make every subject of a DBS Disclosure aware of the existence of the DBS Code of Practice and make a copy available on request.

CSM is committed to ensuring that all information provided about an individual's criminal convictions, including any information released in Disclosures, is used fairly and stored and handled appropriately and in accordance with the provisions of the Data Protection Act 1998. Data on file about an individual's convictions will be held only as long as it is required for employment purposes and will not be disclosed to any unauthorised person.

Having a criminal record will not necessarily bar an applicant from working with us. This will depend on the nature of the position and the circumstances and background of the offences concerned.

5. WHISTLEBLOWING POLICY (CHIME)

Introduction:

The Group is committed to working in an open and accountable manner and wishes all members of staff to know that, should they

become aware of malpractice or impropriety, they can voice their concerns in a responsible and effective manner. This document details the kind of issues that might fall under the scope of “whistleblowing”; outlines the avenues available to you in order to raise your concerns, and confirms that you should not feel at a disadvantage in raising those legitimate concerns.

Audience: For all staff irrespective of location, brand or division and externally, for third parties requiring evidence of our approach and arrangements.

It is the duty of every member of staff to speak up about genuine concerns in relation to:

- Financial malpractice or impropriety or fraud;
- Failure to comply with a legal or regulatory obligation or statutes;
- Dangers to Health & Safety or the environment;
- Criminal activity;
- Improper conduct or unethical behaviour;
- Non-compliance with the Code of Conduct or a serious disregard to Chime’s Values – Score;
- Failure to meet our obligations to clients under our contracts with them, and
- Attempts to conceal any of these.

The Company is committed to investigating your concerns fully.

This procedure is not a channel for you to raise matters relating to your terms and conditions of employment; to reconsider matters which have already been addressed under the disciplinary or grievance procedures; or to question legitimate business decisions made by the Company.

Protection for Whistleblowers

The UK’s Public Interest Disclosure Act (1998) gives legal protection to employees against being dismissed or penalised by their employers as a result of publicly disclosing the kind of serious concerns detailed above. Chime is committed to offering the same protection to employees based or domiciled overseas. You will not be at risk of losing your job or suffering retribution or harassment in disclosing your concerns in line with procedure outlined in this policy, provided that you have raised the matter internally and given the company a chance to investigate and respond and you have reasonable grounds to believe that the disclosure tends to show malpractice or serious impropriety. Even if an investigation reveals that the alleged malpractice or impropriety did not occur, provided that you have followed the procedure, no action will be taken against you.

This policy does not protect someone making malicious or vexatious allegations. It is a term of your employment that you will not disclose confidential information about your employer’s affairs and internal disciplinary procedures would apply where someone chose not to follow the “whistleblowing” procedures and instead disclosed their concerns publicly as a first resort.

The Company is committed to treating your disclosures in a confidential and sensitive manner and will, at your request, keep your identity confidential. If your concern cannot be dealt with without revealing your identity, there will be a discussion as to whether and how we can proceed. You should be aware that you may need to provide a statement in evidence in order for the appropriate action to be taken.

Where information about malpractice or wrongdoing is received anonymously the company will investigate to the best of its ability under the circumstances.

Procedures for making a disclosure

We hope that, in the first instance, you will feel able to raise a concern with your line manager or a director of the company or division for which you work. You can do this verbally or in writing. If the matter cannot be investigated and resolved to your satisfaction by the manager you approach, a senior manager who is not connected to the allegation will be nominated to investigate your complaint.

If, for whatever reason, you feel you cannot raise your concern directly with your line manager or director or if, having done so, you feel your concern has not been handled properly, then you should contact Chime Central:

Bob Davison	Company Secretary	+44 (0)20 7096 5860
Kate Fraser	Head of HR	+44 (0)20 7096 5855

You can also contact Kate or Bob in advance of formally making a disclosure for advice on the implications of the “whistleblowing” legislation and the possible internal and external avenues of complaint open to you.

Confidential Helpline

The Company has also established a helpline to enable employees to speak confidentially to an independent third party about their concerns. This service is provided by EXPOLINK, a leading provider of Whistleblowing helplines used by many of the top companies in the UK and abroad. Employees may call EXPOLINK on 0800 374 199 quoting “CHIME” to report concerns. If you are outside of the UK, a list of alternative freephone numbers is available. The service is free, confidential and available 24 hours a day,

7 days a week and can be used irrespective of time zone. EXPOLINK has multi-lingual consultants on hand to answer calls.

The service is designed to enable employees to report issues such as criminal activity, fraud, theft by the Company, its management, employees or suppliers. It is also available to employees who feel they have been subject to discrimination, bullying or harassment. The calls will be received by impartial staff trained to handle these types of calls and may, if necessary, be made anonymously.

The information given will be passed on one of the senior executives at Chime who will act on it without compromising the caller.

Where there is no Freephone number please communicate the following: Collect call/reverse charge number steps as follows:

- Caller dials their country operator
- Asks for an international collect call or reverse charge to: 0044 1249 661808
- Operator will dial the number and speak to an Expolink Operator who will accept the call and charges
- Country operator connects caller to Expolink, leaves the call and then the call takes place as normal

How we will handle the matter

Once the Company is aware of your concern, we will:

- Check that we have full details and clarification of the allegation you are making.
- Look into the allegation to assess what action should be taken as a first step. You may be asked how you think the matter might best be resolved. If your concern falls more properly within the Company's grievance policy we will tell you this.
- Tell you who your point of contact will be and whether your further assistance may be requested.
- Investigate the matter thoroughly and carefully. Where the complaint is against a specific employee, the employee will be informed of the complaint as soon as practically possible and he/she will be informed of his/her right to be accompanied at any future interviews held to further investigate.
- Consider the involvement of the Company auditors, internal auditor and the Police, if appropriate.
- Form a view as to the validity of the complaint and detail this in a written report for the Chief Executive or Chairman of your Division or of Chime as appropriate
- The Chief Executive/Chairman will decide what action to take. If your complaint is shown to be justified, the disciplinary procedure may be invoked.
- We will give you as much feedback as we can on the outcome of the investigation into your allegations, but we may not be able to tell you the precise action we take where we would be in breach of our duty of confidentiality to someone else.

If you remain unhappy with the outcome

While we cannot guarantee that we will respond to all your concerns in the way that you might want, we are committed to handling your disclosures under the "whistleblowing" policy fairly and properly. If you are not satisfied that your concern has been properly dealt with, you can raise your concern in confidence with the Chief Executive/Chairman of Chime. If the decision on what actions to be taken has already been made by the Chief Executive/Chairman of Chime and you are still unhappy with the outcome, you should raise your concerns with the senior Non-Executive Director of Chime.

If you remain unhappy with the outcome after all internal procedures to deal with your concerns have been exhausted, the Company recognises your lawful right to make disclosures to prescribed agencies such as the Health and Safety Executive, the Financial Services Authority or similar regulatory body.

Note for employees based outside of the UK

Whilst UK legislation may not grant rights to foreign nationals based overseas and may grant other rights via local legislation; the intention of the Company is to provide a framework where employees may voice their concerns in a prescribed manner. As such non-UK workers should adhere to the policy/procedure as above. Where local legislation differs that should obviously take precedence for that part of the policy where any such conflict exists.

6. DATA PROTECTION POLICY

Policy Statement

CSM collects and uses information about people with whom it communicates. This personal information must be dealt with properly and securely however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material – and there are safeguards to ensure this is done in accordance with the UK Data Protection Act 1998 (**Act**) (and other equivalent services for staff/roles based outside of the UK). CSM regards the lawful and correct treatment of personal information as very important to the successful and efficient performance of its functions, and to maintain confidence between those with whom it deals. To this end CSM fully endorses and adheres to the Principles of Data Protection, as set out in the Act.

Purpose

The purpose of this policy is to ensure that the staff, volunteers and trustees of CSM are clear about the purpose and principles of Data Protection and to ensure that it has guidelines and procedures in place which are consistently followed.

This policy is not part of your contract of employment and we may amend it at any time. However, it is a condition of employment that employees and others who obtain, handle, process, transport and store personal data will adhere to the rules of the policy.

Failure to adhere to the Act is unlawful and could result in legal action being taken against CSM or its staff, volunteers or trustees and any breach of this policy will be taken seriously and may result in disciplinary action.

Alexandra Scudamore, Group Legal Counsel, is our Data Protection Officer and responsible for handling any queries you might have about Data Protection.

Principles

The Act regulates the processing of personal data relating to living and identifiable individuals (data subjects). So, lists of contacts, our personnel files, client databases, HR records and even emails with people's names in them will be "personal data". Processing includes the obtaining, holding, using, accessing, disclosing, destroying and almost every other way you might handle personal data. It covers computerised records (on a computer or server) as well as manual filing systems and card indexes. Data users must comply with the data protection principles of good practice which underpin the Act. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

To do this CSM follows the eight Data Protection Principles outlined in the Act, which are summarised as follows:

- Personal data will be processed fairly and lawfully;
- Data will only be collected and used for specified purposes;
- Data will be adequate, relevant and not excessive;
- Data will be accurate and up to date;
- Data will not be held any longer than necessary;
- Data subject's rights will be respected;
- Data will be kept safe from unauthorised access, accidental loss or damage; and
- Data will not be transferred to a country outside the European Economic Area (**EEA**), unless that country has equivalent levels of protection for personal data.

The principles apply to "personal data" which is information held on computer or in manual filing systems from which they are identifiable. CSM's employees, volunteers and trustees who process or use any personal information in the course of their duties must ensure that these principles are followed at all times.

Procedures

The following procedures have been developed in order to ensure that CSM meets its responsibilities in terms of Data Protection. For the purposes of these procedures data collected, stored and used by CSM falls into two broad categories:

- **CSM's Internal data records:** Staff, volunteers and trustees.

- **CSM's External data records:** Members, customers, clients.

CSM as a body is a "data controller" under the Act, and CSM's Group Operations Team is ultimately responsible for the policy's implementation.

Internal data record purposes

CSM obtains personal data (names, addresses, phone numbers, email addresses), application forms, and references and in some cases other documents from staff, volunteers and trustees. This data is stored and processed for the following purposes:

- Recruitment;
- Equal Opportunities monitoring;
- Volunteering opportunities;
- To distribute relevant organisational material (e.g. meeting papers); and
- Payroll.

Sensitive Data

We should not process (e.g. by recording it on our systems) 'sensitive personal data' without the explicit consent of the individual to whom the data relates. This means we need to exercise particular caution where we record (in databases or elsewhere) this data. Sensitive personal data is data concerning an individual's:

- racial or ethnic origin;
- political opinions;
- religious or similar beliefs;

- trade union membership;
- physical or mental health;
- sexual life;
- commission (or alleged commission) of an offence; or
- involvement in proceedings for an offence or alleged offence.

External data record purposes

CSM obtains personal data (such as names, addresses, and phone numbers) from members/clients. This data is obtained, stored and processed solely to assist staff and volunteers in the efficient running of services. Personal details supplied are only used to send material that is potentially useful. Most of this information is stored on the organisation's database.

CSM obtains personal data and information from clients and members in order to provide services. This data is stored and processed only for the purposes outlined in the agreement and service specification signed by the client/ member.

Consent

Personal data is collected over the phone and using other methods such as email. During this initial contact, the data owner is given an explanation of how this information will be used. Written consent is not requested as it is assumed that the consent has been granted when an individual freely gives their own details.

Transferring Data

Personal data will not be passed on to anyone outside the organisation without explicit consent from the data owner unless there is a legal duty of disclosure under other legislation, in which case the Director will discuss and agree disclosure with CSM's Group Operations Team. Ensure that if a third party (e.g. a regulator) asks you for personal data that you are sure they are who they say they are. What checks have you done to ensure this and keep a record of this? If in doubt, ask the firm's Data Protection Officer before sending the requested data.

Contact details held on the organisation's database may be made available to groups/ individuals outside of the organisation.

Transferring personal data to third parties without the appropriate consent of that individual or, if the third party is an outsourced service supplier, without having a written contract in place with the supplier and without having conducted appropriate due diligence on the supplier's own data security measures is likely to amount to a breach of the Act.

International Transfers

Personal data can be transferred freely within the organisation to the EU and European Economic Area Countries, but transfers to other countries are generally prohibited unless you have the consent of the individual concerned or certain prescribed safeguards are in place.

If you are planning to send any personal data to a group company outside the EEA and the person who it is about has not either consented to this (impliedly by emailing you) then please consult with the firm's Data Protection Officer before sending it to check the prescribed safeguards are in place.

Access

Only the organisation's staff, volunteers and trustees will normally have access to personal data. All staff, volunteers and trustees are made aware of the Data Protection Policy and their obligation not to disclose personal data to anyone who is not supposed to have it.

Information supplied is kept in a secure filing, paper and electronic system and is only accessed by those individuals involved in the delivery of the service.

Information will not be passed on to anyone outside the organisation without their explicit consent, excluding statutory bodies (e.g. the Inland Revenue).

Individuals will be supplied with a copy of any of their personal data held by the organisation if a request is made. All confidential post must be opened by the addressee only.

Accuracy

CSM will take reasonable steps to keep personal data up to date and accurate. Personal data will be stored for as long as the data owner/ client/ member use our services and normally longer. Where an individual ceases to use our services and it is not deemed appropriate to keep their records, their records will be destroyed in accordance with the Act.

However, unless we are specifically asked by an individual to destroy their details, we will normally keep them on file for future reference. If a request is received from an organisation/individual to destroy their records, we will remove their details from the database and request that all staff holding paper or electronic details for the organisation destroy them. This work will be carried out by the HR Director.

Sending Marketing

We should only send unsolicited direct marketing communications to individuals (including individual named contacts at organisations who are our clients) if they/their employer are: our clients or potential clients and they have provided us with their details in the course of previous negotiations and the marketing we are sending is on the same or a similar topic to the topic they indicated they would be interested in receiving information about previously and, in such cases, we must always provide them with a simple opportunity to opt out from future marketing initiatives.

Note that all individuals have a right under the Act to require us to stop using their address for marketing.

Storage

Personal data may be kept in paper-based systems and on a password-protected computer system. Paper-based data are stored in organised and secure systems. CSM operates a clear desk policy at all times.

Use of Photographs

Where practicable, CSM will seek consent of members/ individuals before displaying photographs in which they appear. If this is not possible (e.g. a large group photo), the organisation will remove any photograph if a complaint is received. This policy also applies to photographs published on the organisation's website or in the Newsletter.

Criminal Records Bureau (Crb)

CSM will act in accordance with the CRB's code of practice.

Copies of disclosures are kept for no longer than is required. In most cases this is no longer than six months in accordance with the CRB Code of Practice. There may be circumstance where it is deemed appropriate to exceed this limit (e.g. in the case of disputes).

Responsibilities of Staff, Volunteers And Trustees

During the course of their duties at CSM, staff, volunteers and trustees will be dealing with information such as names/addresses/phone numbers/email addresses of members/clients/volunteers. They may be told or overhear sensitive information while working for CSM. The Act gives specific guidance on how this information should be dealt with. In short, to comply with the law, personal information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. Staff, paid or unpaid, must abide by this policy.

To help staff, volunteers and trustees meet the terms of the Act, the attached Data Protection/Confidentiality statement has been produced. Staff, volunteers and trustees are asked to read and sign this statement to say that they have understood their responsibilities as part of the induction programme.

Compliance

Compliance with the Act is the responsibility of all staff, paid or unpaid. CSM will regard any unlawful breach of any provision of the Act by any staff, paid or unpaid, as a serious matter which may result in disciplinary action. Any employee who breaches this policy statement will be dealt with under the disciplinary procedure which may result in dismissal for gross misconduct. Any such breach could also lead to criminal prosecution.

Any questions or concerns about the interpretation or operation of this policy statement should in the first instance be referred to the line manager.

Retention Of Data

No documents will be stored for longer than is necessary. For guidelines on retention periods see the Data Retention Schedule.

All documents containing personal data will be disposed of securely in accordance with the Data Protection principles.

Employee Check List for Handling Personal Data

Collecting Data

When collecting personal information about people, always consider:

- Do I really need this information about an individual? Do I know what I am going to use it for?
- Do the people whose information I am holding know I have got it and what it will be used for?
- If I am sure I don't need the information I have, have I checked it is destroyed securely if it contains personal data?

Keeping Data Up To Date

- Am I sure the personal information I have got is accurate and up to date?
- Am I satisfied the information I hold is secure?

- Have I changed my password regularly?
- Are particularly sensitive documents locked away/password protected?
- Who can access the personal data I hold? Everyone in the business or only those with a need to see it?

Passing Data on to Third Parties

- Am I clear on when I can do this?
- Has the person who the data is about consented to this or am I legally obliged to provide the information?

Handling a Data Breach

- Have I informed Alexandra Scudamore, Group Legal Counsel, CSM London, or the Managing Director, CSM Australia, as soon as possible?

7. DATA PROTECTION FACT SHEET

Background

CSM's business requires it to collect and use information about individuals: its own staff and contractors, its clients, and the general public. When this information identifies a living person, even just basic contact details of name and email address, it is "personal data" and by collecting and using it CSM is a "data processor". Most countries where CSM does business have passed laws protecting a person's rights to his or her personal data and imposing duties on data processors to handle the information appropriately. UK and Australian data protection laws are among the strictest. The UK laws apply whenever CSM in London receives personal data about someone - no matter which CSM office has originally collected it.

Policy

To comply with UK law, and as part of conducting business in a fair and ethical way that respects people's rights, CSM has adopted a Data Protection Policy. Everyone must take a few minutes to read the Policy and this Fact Sheet. Our clients expect us to know and comply with data protection requirements as part of doing good business, so it is important for you to understand the basic rules and know what to do if questions or problems arise.

Principles

Compliance with data protection rests on three fundamental principles:

- **Disclosure** - Before collecting and using someone's personal data, you must explain in a clear and simple way to that person why you want the information and what you will do with it.
- **Safeguarding** - You must take appropriate steps to make sure any personal data you receive is properly stored and handled so that it is only used in the way you've disclosed, and is destroyed once it's no longer needed.
- **Consent**– A person must consent to give up personal data. Consent is implied if personal data is provided after you've clearly explained why you want it and what you will do with it. If you want to use that data for any other purpose, you must get explicit consent to do so. It is especially important to have explicit consent for any transfer of data to a third party, particularly when you want to transfer it to someone outside of the European Economic Area. See below for sample wording to agree with the client if you want to cover the broadest possible range of uses.

Some Frequently Asked Questions

I met with a new client to discuss the work I'd be doing. Everyone at the meeting gave me their business cards, so when I went back to the office I thought I'd distribute them to my team so they could log them onto all their phone and computer contact lists. Is there anything wrong with that?

Contact details on business cards handed to you (or sent by text or email) are personal data and technically you need consent to hold and use them. But as a practical matter, when someone freely hands you his or her business card, you can assume you're able to use that information consistent with the way in which it was given to you. If you get business cards as part of a business discussion, consent to use them to do business with that client is implied, meaning it is ok to distribute them to your team so they have them available to work with the client. The team should keep the information on their business phones and computer systems (not on their personal phones).

Unless the person has said otherwise, it would usually be safe to assume that you could pass on the details to other people at CSM interested in doing business with that client. But before giving these contact details to any third parties, or to anyone who wants the information for personal reasons, you would need to go back to that person to ask permission to do so.

Similarly, when CSM starts work on a project for a client, we typically ask for contact details of the people involved so we can put together a contacts list for the project. Any business cards or details we are then given to create and maintain the contacts list are considered to come with consent to use them for that purpose. But this consent doesn't cover passing on the contact lists to other teams within CSM for completely different purposes, or to third parties. You will need to get additional consent from the client to do so.

I work in one of the CSM offices, and have put together a database of workers recruited for a local event we are managing. May other people in my office use that database as a source for recruiting workers for another event?

The database can only be used to recruit for other events if the workers have consented to this. You will need to check what kind of disclosure was given before the data was collected. This disclosure should state clearly that each worker recruited by CSM for this event explicitly agrees that the personal data supplied by the worker to CSM may be used to recruit for other events. If this kind of disclosure wasn't given to the workers at the outset, you will need to go back to each of the workers to get additional consents.

What if another CSM office wants to use the database?

The same principle applies. If the original disclosure didn't cover allowing other offices to use the database, you will need to go back to the workers to get additional consents. The disclosure must clearly state that the worker agrees that personal data supplied by the worker may be shared by CSM with other offices, listing each of the countries where the other offices are located, or purposes of recruiting for other events.

Does it matter if the database is accessible by other CSM offices through the CSM IT system, so long as they don't download or print out the database?

Computer access is considered to be a transfer for data protection purposes. Unless you have agreed with the client that other offices will have access to the database (e.g. to help process payroll) the database should be password-protected so that it cannot be accessed by anyone other than you and the people in your office who need to use it for the purposes for which the workers were recruited.

Assuming that the database was collected on the basis of a statement that "information may be used by other CSM offices for different purposes," does this mean all the CSM offices globally can freely access and use the database?

In order to comply with laws in the UK and in Australia, this statement isn't enough - consent must be based on a more detailed statement about the countries to which the personal data might be transferred, and the possible purposes for which it might be used. You must be especially careful about transferring any data from London to Australia, Asia or the US, so speak to CSM Legal first if you want to do so.

I was emailing everyone on the original database to get their consent for other offices to access the data, and somehow I hit the wrong button and ended up copying everyone in my office on that group email. What should I do?

You must contact the Data Protection Officer so that she can work with you to make sure all appropriate steps are taken. The Data Protection Officer is Alex Scudamore (Email: alexandra.scudamore@csm.com, DD: 0207 096 5861, Mob: 07788 835 1971). If the Data Protection Officer is not available, you should contact Rob Smith (Email: rob.smith@csm.com, M +61 411 39 39 38.

I was attending an event in order to collect information on my Tablet for a client, including contact details of some of the workers. My Tablet was stolen with that information on it! What should I do?

You must contact the Data Protection Officer (or, If the Data Protection Officer is not available, you should contact Rob Smith (Email: rob.smith@csm.com, M +61 411 39 39 38), who will help make sure that the right steps are followed.

Please read the final section of the Data Protection Policy dealing with security breaches.

Before collecting personal data in future, what should I do to make sure it may be used in the most efficient and appropriate way across CSM?

You should consider whether there are any other purposes for which you, or other CSM offices or agencies, might want or need to use the same data - for example, other events managed by your office, or events or campaigns managed by other offices or agencies. You should work with CSM Legal to make sure the disclosure being given to the people from whom you're collecting data is comprehensive and complies with local law. See below for sample wording to agree with the client if you want to cover the broadest possible range of uses.

CSM managed a big sporting event for a client and as part of that we put together a spreadsheet with contact details for everyone involved in the event from their side. What happens to this spreadsheet when the project is over?

Contact details are personal data. When they are no longer needed for the original purpose, the data must be disposed of properly. Generally, data obtained from the client should either be returned to the client or deleted by the team from their systems once there is no further need for it.

CSM's standard client terms state that CSM will decide whether to return or to delete information (and when to do so), unless otherwise agreed with the client, and also state that CSM, like other companies, runs automated back-up archiving systems which aren't capable of deleting one specific set of files. However, sometimes clients ask for special treatment. For example, some clients will ask that you keep the data for a certain number of years after the project is over, and you will then need to make sure it is stored in a safe place until that time is up. In other cases, clients may ask for confirmation either from CSM or from the client's auditors that the information has been safeguarded throughout the project and then has been wiped from our systems (although please be mindful that data held electronically in back-up form cannot be permanently deleted). You should check with CSM Legal at the beginning of the project to make sure you cover any special data protection requirements. Otherwise, you should use a

common team folder to hold the data during the course of the project, and then close it down and archive it when the project is finished. Contact the IT team if you need any help with this.

Sample Wording

To obtain the client's consent to the broadest possible use of personal data received from the client, the following wording must be agreed with the client. Please speak to CSM Legal before providing this to clients:

In order to carry out business for the client in the best and most efficient way, CSM may wish to share information provided by the client within CSM and with selected third parties. This may include transfer of personal data to CSM offices and suppliers both within, and outside the European Economic Area, in particular to CSM offices in Australia, Asia and the US. CSM will transfer personal data to its offices and to third parties outside the EEA only based on assurances from such offices and parties that appropriate technical and organizational measures are taken against unauthorized or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, the Personal Data, and to protect the security of the Personal Data at all times. By signing this agreement, the client expressly consents to CSM's transfer of Personal Data as set forth above.

8. CRIMINAL RECORDS DISCLOSURE INFORMATION – POLICY AND PROCEDURE

Introduction

CSM has to assess from time to time the suitability of prospective applicants or existing employees for certain types of work where such a person occupies a position of trust. CSM may ask such applicants to submit disclosure applications to the Disclosure & Barring Service (**DBS**) (or other equivalent services for staff/roles based outside of the UK) for the purpose of these assessments. This policy sets out how CSM will handle the results of those assessments (Disclosures and Disclosure Information) and reflects the DBS Code of Practice on the correct handling, use, storage, retention and disposal of the results of Disclosures and Disclosure Information as well as the Data Protection Act and other relevant legislation.

Audience: All staff. This policy may be copied to third parties to evidence our policy.

Correct Handling, Use, Storage Retention and Disposal

Handling

Disclosure information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom Disclosures or Disclosure information has been revealed. It is a criminal offence to pass this information to anyone who is not entitled to receive it.

Usage

Disclosure information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

Storage and Access

Disclosure information should be kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.

Retention

Once a recruitment (or other relevant) decision has been made, we do not keep Disclosure information for any longer than is necessary. This is generally for a period of up to six months, to allow for the consideration and resolution of any disputes or complaints. If, in very exceptional circumstances, it is considered necessary to keep Disclosure information for longer than six months, we will consult the DBS about this and will give full consideration to the data protection and other rights of the individual before doing so. Throughout this time, the usual conditions regarding the safe storage and strictly controlled access will prevail.

Disposal

Once the retention period has elapsed, we will ensure that any Disclosure information is immediately destroyed by secure means (e.g. by shredding or pulping). While awaiting destruction, Disclosure information will not be kept in any insecure receptacle (e.g. waste bin or confidential waste sack). We will not keep any photocopy or other image of the Disclosure or any copy or representation of the contents of a Disclosure. However, notwithstanding the above, we may keep a record of the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.

9. IF YOU HAVE QUESTIONS ABOUT ANY OF THESE POLICIES OR ANY OTHER CONCERNS PLEASE CONTACT:

Rob Smith
Managing Director
CSM Australia

E: rob.smith@csm.com

M: +61 411 39 39 38

About CSM

CSM Sport and Entertainment Australia Pty Ltd is a subsidiary of CSM Sport and Entertainment LLP. CSM is a global leader in the business of sport and entertainment and is part of Chime, now owned by Providence Equity Partners. CSM is active in every major sport through world-class services from strategy to execution. The organisation is made up of 14 specialist agencies and operates on every continent with over 800 people across 26 offices in 19 countries.

For more information visit: **www.csm.com**

Information About Chime

Chime is an international communications and sports marketing group, including CSM, in sports and entertainment; the VCCP Partnership in advertising, the Good Relations Group in public relations, Open Health in healthcare communications, Teamspirit a specialist in financial and professional services and CIE our insight and engagement agency. It is listed on the London Stock Exchange.

Chime is made up of five divisions, 56 companies and over 1800 people. We have offices in the UK, France, Germany, Spain, Czech Republic, Slovakia, Russia, Abu Dhabi, Dubai, Qatar, South Africa, China, Hong Kong, Japan, Malaysia, Singapore, Australia, New Zealand, USA, Canada, South America and Brazil.

For more information visit: www.chimeplc.com