Reviewed On	September 2019
Next Review Date	September 2021 or when a change to legislation and guidance occurs. This document remains in force after the review date if it has not been replaced.
Related Policies/Procedures	Acceptable Use of IT, Email and Phone Policy
	Data Retention Guidance
	Information Security Policy
	Internet, Website and Social Media Policy
	Privacy Statements
	Staff Code of Conduct Policy
	Whistleblowing Flowchart
	Whistleblowing Policy
Responsible Function	Quality
Version	2019-2
Overview of Changes	Changes to Freedom of Information information

Organisational Responsibilities

The Board of Directors are responsible for the operational management of Colebrook (South West) Limited's policies and procedures.

The Chief Executive Officer (CEO) is the designated officer, on behalf of the Board of Directors, responsible for the implementation of the policies and procedures across Colebrook (South West) Limited.

Contact Details

Chief Executive Officer	Vicky Shipway
Telephone Number	01752 205210
E-mail	vshipway@colebrooksw.org

Introduction

Colebrook is committed to being transparent about how we collect and use personal data, and to meeting our data protection obligations in accordance with the General Data Protection Regulations (GDPR) and domestic laws. This Policy sets out the Organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

This Policy applies to the personal data of job applicants, employees, workers and Board members, former employees, clients and service users, people providing feedback on our or other organisation's services, hirers and people attending activity sessions. These are referred to in this Policy as individuals.

This Policy is not contractual but indicates how Colebrook intends to meet its legal responsibilities for data protection. We reserve the right to vary, replace or withdraw this policy at any time.

Definitions

"Data" is information which is processed or is intended to form part of a filing system. This applies to electronic or hard copy formats.

"Data Subject" is any identifiable, natural, legal person.

"Personal data" is any information that relates to an individual who can be directly or indirectly identified from that information.

“Processing” is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric and genetic data (where used for ID purposes).

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

Data Protection Principles

Colebrook processes personal data in accordance with the following data protection principles:

- Personal data is processed lawfully, fairly and in a transparent manner
- Personal data is collected only for specified, explicit and legitimate purposes
- Personal data is processed only where it is adequate, relevant and limited to what is necessary for the purposes of processing
- Personal data is accurate, and all reasonable steps are taken to ensure that inaccurate personal data is rectified or deleted without delay
- Personal data is kept only for the period necessary for processing
- Appropriate measures are adopted to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Colebrook tells individuals the reasons for processing their personal data, how we use such data and the legal basis for processing in our privacy notices. Personal data of individuals will not be processed for other reasons.

Colebrook may process special categories of personal data or criminal records data when:

- Processing is necessary to carry out obligations and specific rights of the controller or individual
- Processing is necessary to protect the vital interests of the individual
- Processing is necessary for the purposes of the assessment of the working capacity of the individual
- The individual has given explicit consent to the processing of personal data.

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

Colebrook keeps a record of its processing activities in respect of personal data in accordance with the requirements of the GDPR.

Roles and responsibilities

Data Controller

Colebrook is the Data Controller, the person or organisation that generates, stores and processes data. Colebrook or its staff may from time to time process data which belongs to an external Data Controller and in all such cases an agreement will have been drawn up confirming each party’s role and responsibilities

Data Protection Officer

Colebrook has appointed the CEO as its Data Protection Officer. Their role is to arrange and protect the personal data we process, they will also ensure that, both in the planning and implementation phases of processing activities, data protection principles and appropriate safeguards are addressed and implemented and that records of processing activity are kept. The Data Protection Officer will also ensure that Privacy Impact Assessments are carried out, when necessary.

Their contact details are:
Chief Executive Officer: Vicky Shipway
Telephone Number: 01752 205210
E-mail: dpo@colebrooksw.org

Data Processor

These roles process personal data on behalf of, and further to, documented instruction given by the Data Controller. They are responsible for taking all measures required to ensure their own compliance with data protection legislation, and to immediately inform the Data Protection Officer if they believe that any instruction given would be in breach of data protection legislation.

Processors are not permitted to appoint another processor without prior written agreement from Colebrook. Equally, when we act as a processor we will not appoint another processor without written agreement of the Data Controller we act on behalf of.

Processors may be third party organisations where we have outsourced specific areas of our work and are bound by individual agreements or they may be employees of Colebrook bound by their employment contracts and Colebrook's other Policies and Procedures

Types of Data Held

Personal data gathered during the individual's relationship with Colebrook is held in organisational files (in hard copy and/or electronic format), and on databases used in the organisation. The periods for which personal data is held are contained in our privacy notices to individuals and are also shown in our Data Retention Guidance.

The following types of data may be held on individuals by Colebrook as appropriate:

- Name, address, phone numbers and contact details – for the individual and their next of kin / emergency contact.
- Application forms and other information gathered during recruitment and selection procedures, including references.
- Referral information from individuals or third parties.
- National Insurance numbers, tax codes and hospital numbers
- Terms and conditions of employment, including job and pay details
- Performance management information and information relating to formal processes.
- Medical or health information, including sickness and risk information
- Sickness absence records
- Training and holiday records
- Photographs and CCTV images

Personal data relating to criminal convictions and offences shall be handled with a greater level of protection than that which is applied to standard personal data.

Colebrook will only process criminal records data, e.g. a criminal records check, where there is a legitimate requirement to do so, namely in respect of our duties as an employer. Where there is a legal obligation for us to review or record such data, we may seek to establish the required information from the employee, worker, self-employed person, contractor or any third party.

Where Colebrook becomes aware of criminal convictions and offences related to clients and service users, this will only be recorded if needed to protect the safety of the person concerned, or our staff and volunteers

Individual Rights

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

Individuals have the right to be informed about how Colebrook processes personal data about them and the reasons for processing. Colebrook privacy notices explain what data we collect, how we collect and process it and the lawful bases relied on for processing.

If Colebrook intends to use data already collected for a different reason than that already communicated, we will inform individuals of the new reason in advance.

Subject Access Requests

Individuals have the right to access the personal data held on them by Colebrook.

Further information on how to request access to personal data is available in Appendix 1.

Other Rights

Individuals have a number of other rights in relation to their personal data.

They can require Colebrook to:

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

To ask for any of these steps to be taken, the individual should send their request to the Data Protection Officer. If the response to the request is that Colebrook will take no action, this will be confirmed to the individual in writing.

Data Disclosures

Colebrook may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include, but are not limited to:

- Any employee benefits operated by third parties.
- Individuals with disabilities – whether any reasonable adjustments are required to assist them at work.
- Individuals' health data – to comply with health and safety or occupational health obligations towards the employee.
- Statutory Sick Pay purposes.
- HR management and administration – to consider how an individual's health affects their ability to do their job.
- The smooth operation of any employee pension plan.
- Any situation where an individual may be a risk to themselves or others.
- Any situation where an individual is involved in illegal activity that affects Colebrook as an organisation, a staff member or anyone acting officially on Colebrook's behalf.
- Client / Service User information where contracts with our funders / commissioners require it.

Such disclosures will only be made when strictly necessary for the purpose.

Data Security

Colebrook takes the security of personal data seriously. There are internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not

accessed, except by employees in the proper performance of their duties. More information can be found in our Information Security Policy, Acceptable Use of IT, Email and Phone Policy, Data Retention Guidance and Security Controls Guidance.

Personal data (special category or not) should only be transferred where it is strictly necessary for the effective running of the organisation or to deliver our contracted services. Employees must seek consent from their Line Manager before transferring special category data.

In addition, employees must:

- Ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them
- Ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
- Check regularly on the accuracy of data being entered into computers
- Always use the passwords provided to access the computer system(s) and not abuse them by sharing with people who should not have them
- Use computer screen blanking to ensure that personal data is not left visible on the screen when not in use
- Ensure permissions are in place before photos are taken and / or used publicly
- Ensure CCTV images and recordings are accessed appropriately and stored securely
- Ensure personal data is not kept or transported on laptops, tablets, USB sticks or similar devices, unless authorised by the Line Manager.
- Ensure they operate lawfully within the General Data Protection Regulation.

Where data transfers occur via physical media such as memory cards, USB sticks etc, they must only be dispatched via secure post such as Royal Mail Tracked® or Royal Mail Signed for® or equivalent services of other companies. The use of first or second class Royal Mail is not permitted. The recipient should be clearly stated on the parcel, and the item securely packaged so that it does not break or crack.

The recipient should be informed in advance that the data is being sent, and must confirm safe receipt as soon as the data arrives. The employee responsible for sending the data is responsible for confirming the data has arrived safely.

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

CharityLog Access / Server Restrictions

In addition to password security requiring access to all of our electronic systems; our two key systems for storage and processing of personal data “CharityLog”, our online database, and our organisational server both have additional levels of access security built in to that password to ensure that only relevant staff members can access personal data. These levels of access are regularly monitored to ensure they are up to date.

Data Monitoring

Monitoring will be carried out in order to fulfil our legal and contractual obligations as an employer as well as to aid effective business operations. Monitoring forms part of our contractual obligations to our funders and where it usually includes the processing of individual data, and may intrude on individuals private lives, it will be carried out in accordance with the GDPR, and only when deemed necessary and justifiable for business purposes.

Colebrook will uphold a degree of privacy and where monitoring is required or necessary, individuals will be informed of the extent of any monitoring, together with the reasons why monitoring is taking place. Access to information and data collected will be secure and restricted to authorised personnel.

Further information is available in our Acceptable Use of IT, Email and Phone Policy.

Data Privacy Impact Assessments

Some of the processing that Colebrook carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the Data Protection Officer will carry out a Data Privacy Impact Assessment (DPIA) to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data Breaches

If an employee discovers that data has been lost or is missing, they should refer to our procedure for reporting data breaches, set out in Appendix 2.

International Data Transfers

HR personal data may be transferred to countries outside the European Economic Area (EEA) as part of off-site back-ups for some of our data processors. These countries include India. Data is transferred outside the EEA under the governance of our data processors.

Automated Decision Making

Individuals have the right not to have decisions made about them solely on the basis of automated decision making processes where there is no human intervention, where such decisions will have a significant effect on you.

Colebrook does not make any decisions based on such processes.

Individual Responsibilities

Individuals are responsible for helping Colebrook keep their personal data up to date. Individuals should let their contact at Colebrook know if data changes, for example if an individual moves house or changes their bank details. If the contact is unclear then employees and volunteers should default to HR, all other individuals should contact a member of the team they are working with or the Data Protection Officer.

Individuals may have access to the personal data of other individuals and of our clients in the course of working or volunteering with us. Where this is the case, individuals are required to help meet our data protection obligations to staff and clients.

Individuals who have access to personal data are required:

- to only access data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- to ensure the secure transfer of data (for example by gaining prior authorisation, using postal services as described above and ensuring physical media is encrypted or password protected)
- not to store personal data on local drives or on personal devices that are used for work purposes.

- To report all known breaches of this policy as soon as possible to their line manager, central admin or the DPO.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under our Disciplinary Procedure. Significant or deliberate breaches of this policy, such as accessing personal data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to summary dismissal.

Third Parties, Contractors and Self-employed Persons

If any third party, contractor or self-employed person is found to be failing to meet obligations with data protection laws then we may serve notice on the contract for services.

Serious, deliberate or negligent transgressions may lead Colebrook to terminate the contract for services with immediate effect. In this event, all reasonable steps will be taken to recover and protect the personal data concerned. Where the rights and freedoms of data subjects are likely to be at risk, the data subjects will be notified without delay. This may also constitute a breach requiring reporting to ICO.

Training

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

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

Confidentiality

It is Colebrook's Policy to disclose confidential information within clearly defined limits. These are:

- On a need to know basis where there may be health and safety or other issues or failure to disclose will put others at risk.
- In defined cases (e.g. disciplinary procedures, court orders and statutory requirements).

Induction to the organisation will include Colebrook's Data Protection Policy to ensure employees, volunteers, Board Members and people using our services are aware of their responsibilities and rights in relation to sharing information.

- It is the employee's responsibility to monitor their own and others communication and challenge the sharing of unnecessary information as needed (whether client, business or personally related).
- We recognise that discussions about clients and volunteers enable teams to provide a good service and initials will be used in discussions and minutes to protect identity.
- Employees should not press 'Reply All' to emails containing confidential information.
- Conversations about people involved in our organisation or the running of the business should occur in a confidential setting.
- Data may be shared with commissioners and partners as part of our contractual relationships in line with our current guidelines.
- Information relating to contracts, funding, employment practice or the running of the organisation are confidential.
- Employees use and receive secure email where appropriate.
- Confidentiality agreements will be used with partner agencies to enable the sharing of sensitive business information and joint working.
- Sharing sensitive business information (budgets, staffing etc.) as part of a tender process should be marked 'Commercial In Confidence' and stored as per our Data Protection Policy

- Board Members have responsibility for storing files, information and reports in line with this Policy and agreed procedures.
- Breaches of confidentiality are regarded as serious and will feature in the employment contract for staff, legal agreements with clients and rules for the Board.

Freedom of Information Requests

Colebrook, a not for profit organisation, is a registered society under the Co-operative and Community Benefit Societies Act 2014, is not covered by the Freedom of Information Act, and as such will not respond to any requests received direct from clients, their carers, relatives or friends or third party organisations.

Healthwatch Plymouth, a service delivered by Colebrook under contract with Plymouth City Council, is covered by the Freedom of Information Act and as such will respond to Freedom of Information requests in accordance with the Act and current ICO guidance. Our Freedom of Information Officer details are the same as those shown above for our DPO. Requests should be made to dpo@colebrooksw.org. Any request would be discussed with the Contract Manager at Plymouth City Council at the earliest opportunity.

Colebrook does recognise that funding and commissioning organisations may be subject to the Freedom of Information Act and that we may hold data from time to time, which belongs to them according to the conditions of any contract in place. Where the funding or commissioning organisation receives a Freedom of Information request and asks Colebrook to provide information against that request, we will comply within 14 days, wherever possible, providing that we are satisfied that the information does belong to the requesting organisation. All requests should be made in writing to the CEO.

DBS Certificates

Colebrook complies fully with the Code of Practice regarding the correct handling, use, storage, retention and disposal of certificates and certificate information.

- In accordance with section 124 of the Police Act 1997, certificate information is only accessed by those who are authorised to receive it in the course of their duties. Colebrook will maintain a record of all those staff with certificates and when further information has been revealed.
- Certificate information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

We will keep a record of the date of issue of the certificate, the name of the person, the type of certificate requested, the position for which the certificate was requested, the unique reference number of the certificate and the details of the recruitment decision taken.

Implementation, Monitoring and Review of this Policy

The CEO has overall responsibility for implementing and monitoring this Policy, which will be reviewed regularly following its implementation and additionally whenever there are relevant changes in legislation or to our working practices. Any queries or comments about this policy should be addressed to the CEO.

Any questions or concerns about the interpretation or operation of this Policy should be taken up in the first instance with their line manager. Any employee who considers that the Policy has been breached in any way should raise the matter with the DPO.

Appendix 1 – Subject Access Request Procedure

Introduction

Under the General Data Protection Regulation (GDPR), individuals have the right to receive confirmation that Colebrook processes their personal data, and also a right to access that data so that they are aware of it and are able to verify the lawfulness of the processing. The process for doing so is called a Subject Access Request (SAR), and this document sets out the procedure to be undertaken when such a request is made by an individual regarding data processed about them by Colebrook.

What is personal data?

"Personal data" is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, including the individual's name.

"Special categories of personal data" (sometimes referred to as Sensitive Personal information) includes information relating to:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life or
- sexual orientation.

Procedure

To make a SAR, the individual should complete a Subject Access Request form and send it to the Data Protection Officer. Including specific details of the data being requested will enable a more efficient response from us.

On receipt of a Subject Access Request Form, in some cases, we may ask for proof of identification before the request can be processed. The Data Protection Officer will inform the individual if their identity needs verifying and the documents required.

The Data Protection Officer will then confirm:

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

The Data Protection Officer will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless agreed otherwise. Only personal data relating to the individual who made the request will be released. If the

individual wants additional copies, we will charge a fee, which will be based on the administrative cost to Colebrook of providing the additional copies.

Colebrook will normally respond to a SAR within a period of one month from the date it is received by the Data Protection Officer. In some cases, such as where we process large amounts of the individual's data, we may respond within three months of the date the request is received. The Data Protection Officer will write to the individual within one month of receiving the original request to tell them if this is the case.

We will be unable to supply certain pieces of information, for instance where it is subject to legal privilege or relates to specific business activity. Where this is the case the Data Protection Officer will write to the individual to inform them that the request cannot be complied with, and give an explanation for the reason.

Individuals must inform the Data Protection Officer immediately if they believe that the data is inaccurate, either as a result of an SAR or otherwise. We will write to the individual within one month of receiving the notification, unless the required correction is complex in which we may respond within three months. If the response is that no action will be taken, we will inform the individual of the reasons for this, and of their right to complain to the Information Commissioner.

In the event that inaccurate data was disclosed to third parties, we will inform the third party of the correction where possible, and also inform the individual of the third parties to whom the data was disclosed.

Refusing a SAR

If a SAR is manifestly unfounded or excessive, or repetitive, we are not obliged to comply with it. If an individual submits a request that is unfounded or excessive, or to which we have already responded, the Data Protection Officer will notify the individual that this is the case and whether or not we will respond to it. Alternatively, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. We will inform the individual of their right to complain to the Information Commissioner.

Enforced SARs

Forcing individuals to obtain information about themselves via a SAR, usually in relation to their criminal record, is a criminal offence. No individual will be required to make a SAR to another organisation, e.g. ACRO Criminal Records Office, HM Prison Service, HM Courts and Tribunal Service or the Crown Prosecution Service, in relation to any aspect of their relationship with Colebrook.

In the event we require information about an individual’s criminal record, we will request this information in accordance with our Employment of Ex-Offenders Policy, or through and according to the contract in place to provide support to that person

Subject Access Request Form

You should complete this form to make a subject access request, which means you are asking Colebrook to confirm to you that it processes your personal data, and to obtain access to that data.

1. Your details

Full Name:	
Title:	Date of Birth:
Current Address:	Previous Address if relevant:
Daytime telephone number:	
Email address:	

You will be asked to provide proof of your identity and address. Please refer to guidance notes.

2. Whose information are you requesting? (please tick the relevant box)

My own (please now go to section 4)	
Someone else's (please fill in section 3)	

3. If you are requesting someone else's information, whose is it? (please provide their details)

Full Name:	
Title:	Date of Birth:
Current Address:	Previous Address if relevant:
Daytime telephone number:	
Email address:	

Your relationship to this person: (please tick the relevant box)

Mother	
Father	
Other (please explain)	

You will be asked to provide proof of your entitlement to request information on someone else's behalf.

4. Details of the information you are requesting (please include any known reference/specific identification details of the relevant documents).

5. Proof of Identification and Entitlement

Document(s) supplied as proof of entitlement (see note 4 in the Guidance notes).
Please describe what documents(s) you are providing:

6. How would you like the documents returned to you:

By post to the address given in Question 1	Please tick
Other (please explain)	

7. Submitting the Request Form

Please send the completed Subject Access Request Form and supporting proof of identity to:

Data Protection Officer, Colebrook (SouthWest Ltd), R/o Engage Southwest, St. Levan Road, Milehouse, PL2 3BG

Signature of Applicant:	**Date:**

For Internal Use Only:		
Identification 1:	Type of identification:	Date seen:
Identification 2:	Type of identification:	Date seen:
Date Request Accepted:		
Date Reply Sent (within 30-day deadline):		

Subject Access Request Form - Guidance Notes

These notes accompany our subject access request form. Once a request is received, we will confirm receipt of your request. We will respond within 30 days of your request confirming whether we hold any data and including copies of information relating to your request.

1. Personal Details

Please complete your personal details as requested and if these are likely to have changed since any information was recorded on you.

2. Details of the Information you Require

If the information you require is held in only one place, you are requested to identify that place if you can, for example which Colebrook service have you received.
If there is specific information you are requesting, please can you identify this, for example which documents you are requesting copies of.

3. Proof of Identification

Proof of name and address may be required to ensure we only give information to the correct person. If we need proof then we require an original document showing your name and current address, for example, a driving licence, recent utility bill (less than 3 months old) or bank statement (photocopies are not acceptable). Documents can be brought to the office, or sent to us with the request (and we will return them by first class post). Your application may be delayed if you do not provide satisfactory identification.

4. Proof of Entitlement

Only the data subject has a right to ask to see their own records. We normally expect a subject access request to be made by the data subject themselves; all individuals aged 16 or over should make their own subject access requests if they have the mental capacity to make decisions (mental capacity as defined in the Mental Capacity Act 2005), unless they appoint someone else to make the subject access request on their behalf.
People making subject access requests on behalf of the data subject need to demonstrate that they have the right to do so.

- For a person with mental capacity aged 16 or over, proof of permission to make the subject access request – a signed letter or consent form from the data subject is required (we may contact the data subject for confirmation that we can release the information to you).
- If the person is deceased then the reason for the request and proof of relationship or other evidence will be required such as a copy of the death certificate.
- For a person making a subject access request on behalf of a person lacking mental capacity, then proof of a valid Lasting Power of Attorney, or an Enduring Power of Attorney or proof of Court-appointed Deputyship.

5. Completed forms

You may email your completed Subject Access Request form to dpo@colebrooksw.org.uk with 'Subject Access Request' in the subject line.
Alternatively, please send your request (where relevant) and supporting proof of identity to:
Data Protection Officer, Colebrook (SW) Ltd, R/o Engage Southwest, St Levan Road, Plymouth PL2 3BG.

Appendix 2 – Procedure for Reporting Data Breaches

Introduction

Colebrook is fully aware of its obligations under the General Data Protection Regulation (GDPR) to process data lawfully and to ensure it is kept securely. We take these obligations extremely seriously and have protocols in place to ensure that, to the best of our efforts, data is not susceptible to loss or other misuse.

The GDPR incorporates a requirement for a personal data breach to be notified to the supervisory authority and in some cases to the affected individuals. This procedure sets out Colebrook's stance on taking action in line with GDPR if a breach occurs.

Personal Data Breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed. A 'breach', for these purposes, is identifiable as a security incident which has affected the confidentiality, integrity or availability of personal data.

As indicated above, a data breach for these purposes is wider in scope than the loss of data. The following are examples of data breaches:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a data controller or data processer
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

Breach Detection Measures

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

- IT passwords reset every 3 months
- Charitylog access restrictions administrated by key personnel
- server systems with layered restricted access audited regularly
- all portable equipment with passwords and encryption
- procedure for wiping and resetting equipment
- security audits
- restrictions on the removal of personal data from Colebrook's premises
- clear desk policy
- working from home procedures including staff security measure for home working

We may also become aware of a personal data breach from a member of staff, a client, a volunteer, a member of the public etc.

Notifiable Breaches

All breaches need to be logged internally. For the purposes of this procedure, a data breach will be notifiable to the ICO when it is deemed by Colebrook as likely to pose a risk to people's rights and freedoms. If it does not carry that risk, the breach is not subject to notification although it will still be entered on our breach record.

A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

When assessing the likelihood of the risk to people's rights and freedoms, we will consider:

- the type of breach

- the type of data involved including what it reveals about individuals
- how much data is involved
- the individuals involved e.g. how many are involved, how easy it is to identify them etc
- how bad the consequences for the individuals would be and
- the nature of our work and the resultant severity of a breach.

Reporting a Breach

If an employee identifies a breach of personal data, they must inform their line manager or another manager immediately, who will refer the matter to the Data Protection Officer. An investigation will be initiated to establish the events leading to the breach, and determine what actions should be taken to restrict any consequences. A decision will be taken at that point about whether the breach is deemed notifiable, and whether it is deemed as resulting in a high risk to the rights and freedoms of individuals.

If there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of discovery. If notification is made beyond this timescale, we will provide reasons for this. If it has not been possible to conduct a full investigation into the breach within 72 hours, an initial notification of the breach will be made within 72 hours, giving as much detail as possible, together with reasons for incomplete notification and an estimated timescale for full notification. The initial notification will be followed up by further communication to the Information Commissioner to submit the remaining information.

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

- a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned and
    - the categories and approximate number of personal data records concerned
- the name and contact details of the Data Protection Officer where more information can be obtained
- a description of the likely consequences of the personal data breach and

a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.The Police may also be informed if it is found that unauthorised individuals have unlawfully accessed special category data that has been kept securely within the organisation.

If a notifiable breach has occurred which is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals as soon as possible that there has been a breach and provide them with the following information:

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

A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

Record of Breaches

The Data Protection Officer and / or administrative support will record all personal data breaches regardless of whether they are notifiable or not, as part of our general accountability requirement under GDPR. We will record the facts relating to the breach, its effects and the actions taken.