DATA PROTECTION POLICY

Review Schedule	
Created:	September 2016
Reviewed:	April 2017
Approved by Trustees:	20th July 2017
Reviewed:	July 2018
Approved by Trustees:	20/07/2018
Reviewed:	June 2019
Approved by Trustees:	19/07/2019
New Review Due:	June 2020
Reviewed:	01/06/2020
Approved by Trustees:	05/06/2020
Next Review Due:	June 2021
Reviewed:	24/08/2021
Approved by Trustees:	15/10/2021
Next Review Due:	October 2022
Reviewed:	25/11/2022
Approved by Trustees:	22/12/2022
Next Review Due:	November 2023
Reviewed:	27/09/2023
Approved by Trustees:	13/12/2023
Next Review Due:	September 2024
Reviewed:	September 2024
Approved by Trustees:	September 2024
Next Review Due:	September 2025

CONTENTS: Page no.

1.0 PURPOSE

Safeline is fully committed to protecting personal data and complying with all data protection obligations as set out by the Data Protection Act 2018.

Safeline has a legal basis for processing certain data about its clients, staff, volunteers, partners and stakeholders. Safeline understands that it has a legal obligation to protect the personal data it holds and to ensure that appropriate security measures are in place to safeguard the integrity and security of that data.

The purpose of this policy is to outline how Safeline gathers, handles and retains its data in accordance with organisational standards and legal compliance (Data Protection Act 2018).

The purpose of this policy is to:

- Safeguard an individual's data rights
- To offer transparency and clarity regarding data processing so individuals understand what happens to their data from the point of capture
- To inform and educate the Safeline team about their responsibilities in relation to data protection
- Protect Safeline from breaches of confidentiality – e.g. information being given out inappropriately
- Limit reputational damage – e.g. Safeline could suffer if an unauthorised source successfully gained access to personal data.

2.0 SCOPE

This policy applies to Safeline employees, volunteers, clients, partners, stakeholders, contractors and suppliers. It applies to all data collected and processed within Safeline, whether electronic or written form, or other material, relating to identifiable individuals.

Safeline Data Protection Policy is operated in accordance with the laws of England and Wales.

3.0 DEFINITIONS

3.1 **DATA PROTECTION:** the legal control over access to and use of data.

3.2 **DATA:** Information which is collected, processed or recorded about a **data subject** (i.e. client, employee, donor, supplier). This data can be in both written and electronic form and held in a structured and systematic format (i.e. filing system/database).

3.3 **PERSONAL DATA:** Information relating to an identifiable person i.e. name, address, identification number, location data, online identifier (i.e. web analytics), IP address, photo, CCTV, expression or opinion.

3.4 **SPECIAL CATAGORIES OF PERSONAL DATA:** Racial, ethnic origin, political opinions, religious beliefs, trade union membership, genetic and biometric data, health, sexual orientation, all of which are deemed sensitive and are granted greater protection due to the risk to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

3.5 **DATA CONTROLLER:** The person who, either alone or with others, decides what personal information Safeline will hold and how it will be used.

3.6 **DATA PROCESSOR**: any person who processes the data on behalf of the data controller.

3.7 **DATA PROCESSING:** means collecting, amending, handling, storing or disclosing personal information.

4.0 RESPONSIBILITIES

4.1 The Data Protection Officer, currently the CEO, is responsible for:

- Briefing the Trustee Board on data protection responsibilities;
- Working in conjunction with the Senior Leadership Team (SLT) to ensure Safeline's legal basis for processing data
- Notifying the Information Commissioners Office (ICO) when there has been a data breach
- Leading with the investigation of a data breach
- Approving unusual or controversial disclosures of personal data
- Approving contracts and data sharing agreements with data processors

- Approving privacy statements
- Working in conjunction with the SLT to determine the need for data impact assessments
- Working in conjunction with department heads to devise procedures (including induction and training) to ensure that good data protection practice is established and followed and ongoing training needs are addressed
- Addressing any data protection queries including those from external media outlets
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles
- Approving any data statements attached to communications such as emails and letters

4.2 The Head of Operational Services is responsible for:

- Reviewing the Data Protection Policy and associated policies annually as agreed
- Working in conjunction with the CEO and colleagues on the SLT to devise operational procedures (including induction and training) to ensure that good data protection practice is established and followed
- Managing the data sharing partnership with Safeline's accountants, HR contractor and IT contractor(s)
- Liaising with Safeline's IT partner's to ensure all systems, operational services and equipment used for storing data meet acceptable security standards
- Liaising with Safeline's IT contractors to confirm regular checks and scans are carried out to ensure security hardware and software is functioning properly
- Evaluating any third-party services that the organisation is considering using to store or process data, for instance, cloud computing services
- Writing data protection statements attached to communications such as emails and letters (prior to CEO approval).

4.3 Senior Leadership Team – each department, where personal data is handled, is responsible for complying with this policy. Heads of departments are responsible for (in relation to their department):

- Identify Safeline's legal basis for processing data
- Ensure each department is fully compliant with its data protection obligations
- Notify the CEO of any changes in their use of personal data that might affect Safeline's legal basis for processing data
- Informing supervisees of their responsibilities in relation to data processing
- Identifying and sourcing any data protection training needs of supervisees
- Investigating any potential data breaches within their department before escalation to the Data Protection Officer where appropriate
- Informing the CEO and SLT of data protection issues
- Handling data subject access requests in relation to their department
- Writing privacy statements (prior to CEO approval) and managing their delivery

- Reviewing privacy statements, when deemed necessary, to ensure they are still fit for purpose
- Writing data sharing agreements with data processors (prior to CEO approval).

4.4 Staff, counsellors, contractors and volunteers – all individuals are required to read, understand and accept any policies and procedures that relate to the personal data they may handle during their work, actively participant in training and to notify their line manager of any suspected data breaches immediately.

4.5 Data Processor - when work is outsourced and involves a contracting organisation having access to personal data, there must be a suitably written contract and Data Sharing Agreement in place. Each party is responsible for ensuring their data protection processes are fully compliant with data protection regulations in accordance with the laws of England and Wales.

5.0 GUIDELINES

5.1 In order to ensure that there is no unauthorised or unlawful processing or disclosure of data, all data is:

- Fairly and lawfully processed
- Obtained only for specific purposes as specified at the point of capture, and not processed in any manner incompatible with those purposes
- Adequate, relevant, accurate and not excessive in relation to those purposes
- Not kept for longer than is necessary
- Processed in line with the data subject's rights under the Data Protection Act 2018
- Not transferred outside the European Economic Area (EEA), unless that country or territory offers an adequate level of protection
- Stored securely and kept by the data controller who takes appropriate measures to protect and prevent any unauthorised or unlawful processing or accidental loss, destruction or damage to personal information.

5.2 Safeline will:

- Comply with both the law and good practice
- Ensure they have identified their legal basis for processing data and have sought a data subject's affirmative and freely given consent where applicable
- Ensure robust procedures are in place to ensure all data is processed lawfully and kept secure
- Train and support staff, counsellors, contractors and volunteers who handle personal data so that they can act confidently and consistently in line with organisational policy
- Ensure only authorised people who need to access data for their work are granted access. Data will not be shared informally, internally or externally to non-authorised people
- Respect individuals' rights, and be open and honest with individuals whose data it holds

- Deal courteously and in line with ICO guidelines with any data subject access request and any enquiries about handling personal information
- Where applicable, ensure data is protected using encryption software/strong passwords which are not circulated
- Ensure that such data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects regarding the processing of personal information
- Ensure data is regularly reviewed and updated and deleted or responsibly disposed of if no longer required or out of date
- Provide Safeline clients and personnel clear information about why data is collected and how it is stored so that they can give informed consent
- Encourage staff to ask for help if unsure of their data protection responsibilities
- Instruct staff to contact Safeline's IT contractors and line manager immediately if they suspect there has been a system compromise or a data breach
- Ensure data is only shared/accessed by authorised parties.
- Ensure that the data protection rights of the data subject are explained fully, clearly and in an age-appropriate way.

6.0 DATA COLLECTION

6.1 The data Safeline collects and retains must be deemed necessary for the successful operation of the organisation. Examples of the data we collect include service users contact details, case notes, HR records or data needed to achieve organisational aims such as supporters' information.

6.2 Data may be held for the following purposes:

- Service delivery
- Employee administration
- Fundraising
- Achieving the objectives of a charitable organisation or voluntary body
- Accounts & records
- Advertising, marketing & public relations
- Research
- Volunteers

6.3 When collecting data, either in person or by completion of a form, Safeline will ensure that the data subject:

- Clearly understands why the information is needed and how it will be used. For clients who are accessing Safeline's counselling, Independent Sexual Violence Advocacy support (ISVA) and Prevention Services this will be explained at the point of referral and again during the initial assessment. Clients will be issued a data privacy statement explaining what data is captured, why and how their data is handled and stored. The same process will apply for children aged 13 and upwards. For clients under this age, consent will be sought from a non-

abusing parent or guardian who will be responsible for explaining the implications to the child

- Understands the process should he/she decide not to give consent to processing
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
- Understands that in certain circumstances, under the Data Protection Act 2018, personal data may be disclosed to law enforcement agencies without the consent of the data subject
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- Understands the process to follow if they wish to access their data and how to contact the ICO if they feel their data has been incorrectly or unlawfully processed. This will be explained in a data privacy statement that will be issued.

7.0 DATA STORAGE RULES

7.1 These rules describe how and where data should be securely stored.

7.2 When data is stored on paper, it should be kept in a secure place where unauthorised people cannot access it. This also applies to data that is usually stored electronically but has been printed out.

- Client data should be anonymised via the use of an ID number coding system
- When not required, the paper or files should be kept in a locked drawer or filing cabinet
- Staff should make sure paper and printouts are not left where unauthorised people could see them, i.e. on a printer or desk
- Data printouts should be filed, shredded and disposed of securely when no longer required or when the data retention period has passed.

7.3 When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between persons
- Electronic folders storing data should have limited permissions access
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used
- Data should only be stored on designated drives, servers and cloud-hosted platforms, and should only be uploaded to an approved computing service
- Servers containing personal data should be sited in a secure location, away from general office space (if not cloud-based)
- Data should be backed up frequently. Those backups should be tested regularly, in line with Safeline's standard backup procedures
- Personal information stored on portable devices, such as memory sticks and laptops must be appropriately encrypted and password protected. The use of USBs may be restricted where appropriate and may require authorisation to use

- All servers and computers containing data should be protected by approved security software and a firewall
- All personal and organisational data is non-recoverable from any computer system previously used within Safeline
- Client data should be anonymised via the use of an ID number coding system.

7.4 All client notes including assessment forms, paper or electronic, employee, contractor and volunteer details and financial records will be kept for a period of 7 years and individuals should be informed accordingly. Referral forms from third parties or from clients who do not go on to access services will only be stored for 6 months. Application forms for employment positions will be disposed of immediately if not shortlisted. Shortlisted application forms will be stored for no longer than 6 months.

7.5 Data protection procedures apply to office-based and remote/external working. If a Safeline employee, contractor or counsellor is carrying out Safeline work from a remote, external location (including homeworking), they are expected to understand and follow the advised guidelines at all times. Wherever possible and practical, Safeline personnel will be given the equipment needed to work remotely which is to be used by the intended user only. If using non-Safeline issued equipment, the user is responsible for ensuring appropriate anti-virus and security software is in place before any Safeline work is carried out. No data is to be stored on non-Safeline issued equipment. When using a telephone/mobile phone to contact clients, all data should be removed immediately, and no data is to be stored on the equipment. Any hard copies of data should be kept in a lockable storage facility and returned to the office as soon as possible. This storage facility should only be accessed by the authorised person.

8.0 IT SECURITY

8.1 All data stored within the IT platform meets a high level of security standards. Safeline's IT system runs from a core infrastructure that sits within a secure tier 3 enterprise grade data centre, which is fully accredited to all data centre standards. The services are monitored to detect possible service security breaches. All user end points that access the service are protected with antivirus protection and sit behind a hardware firewall.

8.2 Safeline's IT systems are cloud hosted. Any remote access is fully protected as the service runs from a datacentre and only the image viewed is transmitted to the local device. Our IT system protects the organisation from any data being saved on local devices with the ability to lockdown external drive access and local drive access to stop users from saving data to their local machines.

8.3 Safeline has security patches in place which target any security vulnerabilities and uses software which highlights if there are patches pending and need to be installed.

8.4 The datacentre is SS AE16 compliant and ISO 27001, ISO 14001 and ISO 9001 accredited through the landlord Digital Realty Trust. The supplier supports customers in a variety of industries, which must abide by multiple security

standards including PCI, HIPPA, SSAE 16, ISO17799:2000, ISO/IEC TR14516, ITIL, SOX.

8.5 Safeline's IT contractors are trained in data protection processes and confidentiality and are compliant with both data protection legislation and good practice. A data sharing agreement is in operation between both parties.

9.0 DATA TRANSMISSION

9.1 When data is transmitted as part of the therapeutic or emotional support process, for example, in online or telephone counselling or in helpline and online support work, care must be taken to safeguard the client:

- Safeline will offer a clear informed consent process where information on services available and access to services is available via the website and in discussion with Safeline staff;
- Safeline will offer clients the information they need to give informed consent. They will be asked what method of communication they prefer to use to access Safeline services, for example, information about which methods of communication are encrypted;
- Methods of data transmission will be protected by strong passwords that are changed regularly and not circulated electronically;
- It is against Safeline's policy to transfer passwords electronically. Passwords should be communicated via telephone or in person.
- Interactions where data is transmitted will only take place via approved methods and platforms;
- Clients will be given clear information about the records Safeline collects relating to its services in the form of a data privacy statement.
- If carrying out data migration, a full Data Impact Assessment will be performed, outlining levels of risk and identifying mitigating actions. This assessment will be carried out in advance of any data being migrated.

10.0 DATA USE

10.1 It is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure their computer screens are always locked when left unattended;
- Personal data should not be on display and be shared informally;
- Wherever possible, data should be encrypted before being transferred electronically;
- Personal data should never be transferred outside of the European Economic Area, unless that country or territory offers an adequate level of protection;
- Employees should not save copies of personal data to their own computers, but always access and update the central copy of any data;
- Data should be held in as few places as possible and updated regularly.

11.0 DATA BREACHES

11.1 Safeline understands a data breach to be:

"A security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed." *Source: ICO*

11.2 Safeline will follow the guidelines as set out by the ICO in reporting data breaches, where a report will be filed with the ICO if Safeline has identified that a breach may cause severe risk to people's rights and freedoms.

11.3 In this event, the CEO will notify the ICO of a data breach within the 72 hours advised timeframe and notify Safeline's Trustee Board and all individuals whose data was breached promptly.

11.4 A review of Safeline's data protection processes and security measures will be carried out immediately.

12.0 DISCLOSURE

12.1 Safeline may share data with other agencies such as the local authority, funding bodies and other voluntary agencies. Unless Safeline is instructed to share this data by law, the data subject will be made aware of how and with whom their information will be shared.

12.2 There are circumstances where the law allows Safeline to disclose data (including special categories of personal data) without the data subject's consent. Under these circumstances, Safeline will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the organisation's legal advisers where necessary. These circumstances are:

- Carrying out a legal duty or as authorised by the Secretary of State;
- Protecting vital interests of a data subject or other person;
- The data subject has already made the information public;
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights;
- Monitoring for equal opportunities purposes – i.e. race, disability or religion;
- Providing a confidential service where the data subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing a stressed or unwell data subject to provide consent signatures.

13.0 DATA SUBJECT ACCESS REQUESTS AND ACCURACY

13.1 All data subjects are entitled to be informed about:

- What information Safeline holds about them and why Safeline is processing their data;
- How to gain access to it;
- How to keep it up to date;
- The length of time it will be stored for;
- The lawful circumstances in which their data may be shared;
- How Safeline is meeting its data protection obligations;
- How to complain if they believe their data has been unlawfully or incorrectly processed.

13.2 An individual has the right to receive confirmation that their own personal data is being processed. They can also request a copy of the personal data that is held relating to them, known as a subject access request. Safeline understands that it has a legal obligation to handle subject access request accordingly.

13.3 Safeline understands that subject access requests relate to the data held at the time the request was received. If a large amount of data is held about an individual, we may need to ask for more information in order to clarify the request.

13.4 Subject access requests can be made in either written or verbal form and the requests do not have to be made to a specific person within the organisation.

13.5 An individual can make a request via a third party. In these cases, Safeline will need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of this entitlement.

13.6 The data controller will always verify the identity of anyone (including third parties) making a subject access request before handing over any information. All subject access requests will be recorded on file.

13.7 In response to a valid subject access request, the data controller will provide the relevant data within one calendar month starting the day after the of receipt of the access request. Safeline has the right to exceed the response time by a further two calendar months if the request is complex or we have received multiple requests from the same individual. Safeline may charge a reasonable administrative fee if the request is deemed excessive or unfounded.

13.8 Data may be provided electronically or in hard copy format.

13.9 The data controller may withhold certain data, including some third-party material, if a duty of confidentiality is owed to the third-party. Third-party means either that the data is about someone else or someone else is the source.

13.10 It may be that very occasionally a client is very mentally unwell and reading the information about a traumatic past may present a real concern of a deterioration or harm. Due care should be taken when giving a client a copy of their notes to ensure they have suitable support in place. In rare circumstances, the organisation may seek legal and professional advice if there are concerns that

releasing personal information to a client about themselves may cause significant harm to the individual's mental or physical health. Exemptions under Part 5 Schedule 3 relating to the maintenance of confidentiality of child abuse data may also apply.

13.11 Any data subject request for their data to be deleted is assessed on a case-by-case basis in accordance with the legislation as outlined in the Data Protection Act of 2018.

14.0 TRAINING

14.1 Everyone processing personal data will be appropriately trained. New employees and volunteers will receive appropriate data protection training as part of their induction to explain how they should process personal information. They will be asked to sign a data protection statement, confirming that they understand their responsibilities regarding data protection.

14.2 Counsellors who offer counselling face to face, online or via other distance methods are expected to be appropriately trained in using these methods safely and securely as part of their qualification. Information regarding organisational data protection policies will be shared as part of the induction process.

15.0 ENFORCEMENT

15.1 All staff must be aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them. Significant breaches of this policy will be handled under Safeline's disciplinary procedures.

16.0 MONITORING AND REVIEW

16.1 Safeline will regularly review and audit the ways personal information is gathered, held, managed and used and evaluate its methods and performance in handling personal information.

16.2 This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 2018.

16.3 In case of any queries or questions in relation to this policy please contact the Safeline Data Protection Officer.

17.0 LINKS WITH OTHER POLICIES

- IT Policy
- Confidentiality Policy
- Employee Handbook
- Trustee Handbook

- Volunteers Policy
- Child Protection Policy
- Adults at Risk Policy
- Data Privacy Statement – Employees, Volunteers, Trustees, Client (document)
- Joint Data Sharing Agreement (document)

Appendix 1
Source: ico.org.uk

A QUICK 'HOW TO COMPLY' CHECKLIST

This short checklist will help you comply with the Data Protection Act (2018). Being able to answer 'yes' to every question does not guarantee compliance, but it should mean that you are heading in the right direction.

- Do I really need this information about an individual? Do I know what I'm going to use it for?
- Do the people whose information I hold know that I've got it, and are they likely to understand what it will be used for?
- Am I satisfied the information is being held securely, whether it's on paper or on computer? And what about my website? Is it secure?
- Am I sure the personal information is accurate and up to date?
- Do I delete/destroy personal information as soon as I have no more need for it?

- Is access to personal information limited only to those with a strict need to know?
- If I want to put staff details on our website have I consulted with them about this?
- If I use CCTV, is it covered by the Act? If so, am I displaying notices telling people why I have CCTV? Are the cameras in the right place, or do they intrude on anyone's privacy?
- If I want to monitor staff, for example by checking their use of email, have I told them about this and explained why?
- Have I trained my staff in their duties and responsibilities under the Act, and are they putting them into practice?
- If I'm asked to pass on personal information, am I and my staff clear when the Act allows me to do so?
- Would I know what to do if one of my employees or individual customers asks for a copy of information I hold about them?
- Do I have a policy for dealing with data protection issues?
- Do I need to notify the Information Commissioner?
- If I have already notified, is my notification up to date, or does it need removing or amending?

Appendix 2

Safeline Data Protection Statement

I understand that as an employee of Safeline I have a responsibility for ensuring that data is processed lawfully at all times.

I understand that I am required to complete data protection related training, read, understand and accept any policies and procedures that relate to the data I may handle in the course of my work. I understand that a breach of Safeline's data protection procedure may lead to disciplinary action being taken.

If you have any questions regarding Safeline's Data Protection Policy, please speak to your line manager.

Employee Name: .....

Employee Signature: .....
Date: ……

Appendix 3

System Compromise or Suspected Data Breach Internal Process

If you suspect your system or data in your care has been compromised, it is important you act promptly and in line with Safeline's protocol.

Safeline understands a data breach to be:

"A security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed." *Source: ICO*

There may be a number of mitigating factors to consider in a data protection situation, so it is important to liaise with your line manager as soon as you are aware of a potential compromise or breach so it can be appropriately internally investigated.

Suspected Data Disclosure

- If you suspect there has been a potential data compromise or breach, you have a responsibility to notify your line manager immediately. This may include, but not limited to, the sending of personal data to an incorrect person, lost paperwork, an incorrect disclosure, the destruction of data.
- Your line manager will then work alongside you to investigate if a breach or compromise has occurred and assess what action needs to be taken.
- To assist with this process, it is important to provide as much detail to your line manager as possible, including the background that has led to the present situation, who was involved and timeframes. It is important to be as honest as possible, even if you are worried you have made a mistake, to limit the impact of the disclosure.

Suspected IT System Compromise:

If you suspect your IT system has been maliciously compromised, all users have a responsibility to contact Safeline's IT partners immediately. Acting promptly can help reduce the potential impact and provide a clearer picture of the type of breach that has occurred.

You need to provide as much detail to our IT partners as possible, including the unusual activity you have detected, dates, timeframes and the background that has led to the present situation. It is important to be as honest as possible, even if you are worried you have made a mistake, to safeguard against the impact spreading across the organisation.

If you are a fellow IT user and have received a suspicious looking email purporting to be from your colleague or a known contact, do not respond to the email. Contact the sender on another channel (phone or in person) to ask if it has been genuinely sent by them. If not, contact IT immediately who will advise you on the next steps to take.

Inform your line manger immediately regarding what has happened and the actions you have taken.

It is the line manager's role to:

- Liaise with IT to understand what areas of the system have been compromised and to authorise the necessary user account password resets.
- Decide what immediate communication needs to be sent to wider team to safeguard against the compromise internally spreading.
- Lead with the internal investigation to understand what has happened.
- Be the point of contact with IT during the internal investigation.
- Once a report from IT has been received, review this report to assess what personal data, the quantity, has been maliciously accessed.
- Contact the Information Commissioner's Officer for advice if deemed necessary.
- Decide who within the affected employee(s) contacts list need to be made aware.
- Work alongside the CEO, Safeline's Data Protection Officer, IT partners, data protection partners and fellow department heads to assess if a data breach has occurred and the level of impact on those affected. If a breach has occurred, liaise with Safeline's Data Protection Officer and notify the Information Commissioners Office within the specified timeframe.
- Retain a log of the steps taken during the internal investigation process, including collating evidence as part of an audit trail.
- Stay in regular contact with the affected employee(s) so the right action can be taken, the necessary information can be obtained in a timely manner and support can be given to the individual where needed.
- Work alongside the CEO, Safeline's Data Protection Officer, fellow department heads and Safeline's IT partner's to assess what additional security measures, training needs or process reviews needs to be put in place going forward.

If the breach has affected multiple departments, department heads are responsible for collectively deciding who will lead with which of the above responsibilities.