Extra Mile Charity

Data Breach Policy

Date Adopted	*August 2018*
Date reviewed by Trustees	*January 27th 2021*
Date of next review	*January 2022*
Chair of Trustees	**Mike Fielding**

Extra Mile Data Breach Policy

February 2021

1. Statement of Intent

1.1 As a UK charity employing individuals in Sierra Leone to improve the life chances of poor children and adults at risk, Extra Mile, through its education, holds large amounts of personal and sensitive data on students, staff, volunteers, donors, trustees, governors and individuals who participate in Extra Mile's fundraising activities

1.2 Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is imperative that appropriate action is taken to minimise any associated risks as soon as possible. This breach procedure applies to all personal and sensitive data held by Extra Mile. This procedure applies to all Extra Mile's employees, volunteers, trustees, governors and contractors working with Extra Mile.

2. Purpose

2.1 This breach procedure sets out the course of action to be followed by employees, volunteers, trustees, governors and contractors if a data breach takes place.

3. Legal context

3.1 Data security is a cornerstone of the current UK General Data Protection Regulation (GDPR) and this is likely to remain as the cornerstone of UK policy in the future. The current sixth data protection principle - the integrity and confidentiality principle - requires Extra Mile to take appropriate technical and organisational measures to protect personal and sensitive data in a manner that ensures appropriate security including protection against: 3.1.1 unauthorised or unlawful processing; and

3.1.2 accidental loss, destruction or damage.

4. Types of Breach

4.1 A personal data breach can be broadly defined as 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.

4.2 Data protection breaches can be caused by a number of factors. Some examples are:

4.2.1 loss of student, staff, volunteer, trustee, governing body, supporters' data and/or equipment on which the data is stored;

4.2.2 inappropriate access controls allowing unauthorised use;

4.2.3 equipment failure;

4.2.4 human error, such as accidental deletion or alteration of data or sending data to the wrong recipient;

4.2.5 unforeseen circumstances such as floods or fire;

4.2.6 deliberate attacks on the system, such as hacking, viruses or phishing scams; and "blagging " offences where information is obtained by deception.

5. Procedures

5.1 Step One: Immediate Containment/ Recovery

5.1.1 On discovery of a data protection breach, the following steps should be followed:

5.1.1.1 Inform the Chairm

- ✓ The individual who discovers/receives a report of breach must immediately (as soon as is practically possible) inform the Chairman.

5.1.2 Containment and Recovery

- ✓ The Chairman or an individual nominated by them must ascertain whether the breach is still happening. If so, steps must be taken immediately to minimise the impact of the breach. An example might be to shut down the system. The Chairman will also immediately inform the police where illegal activity is known or is believed to have occurred, or where there is the risk of an illegal activity happening in the future

5.1.3 Assess and record

- ✓ The Chairman will inform the trustees as soon as possible and undertake a thorough investigation of the breach and enter the breach on the data breach register. It is the Chairman's responsibility to take appropriate action and conduct or oversee the investigation. Further information on investigations can be found in the notes below.

5.1.4 Notify the Information Commissioner's Office (ICO).

- ✓ Notification is not required where the breach is unlikely to result in a risk to the rights and freedoms of individuals. Further information on ICO notification can be found in the Notification section(below).

5.1.5 The Chairman or nominated individual must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

- ✓ attempting to recover lost equipment
- ✓ contacting the relevant staff, volunteers, trustees, governors and contractors, so that they are prepared for any potentially inappropriate enquiries (phishing) for information on the individual or individuals concerned consideration should be given to a universal email to all individuals involved with the charity
- ✓ if an inappropriate enquiry is received by an individual involved with the charity, they should attempt to obtain the enquirer's name and contact details (if possible) and

confirm that they will ring the individual making the enquiry back. Whatever the outcome of the call, it should be reported to the Chairman immediately.

- ✓ using back up facilities to restore lost/damaged/stolen data
- ✓ if bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use
- ✓ if the data breach includes any entry codes or IT system passwords, then these must be changed immediately and any relevant agencies and individuals connected with the charity informed.

6. Step Two: Investigation

6.1 In most cases, the next step would be for the Chairman or nominated individual to fully investigate the breach as a matter of urgency. The Chairman or nominated individual should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigator should consider:

6.1.1 the type of data;

6.1.2 its sensitivity;

6.1.3 what protections are in place (e.g. encryption);

6.1.4 what has happened to the data;

6.1.5 whether the data could be put to any illegal or inappropriate use;

6.1.6 how many individuals affected;

6.1.7 what type of individuals have been affected (students, staff, volunteers, trustees, governors)

6.2 A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency and, wherever possible, within 5 working days of the breach being discovered/reported. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

7. Step Three: Notification

7.1 The charity may have already notified the Information Commissioner's Office and/or police as part of the initial containment. However, the decision to notify the ICO will normally be made once an investigation has taken place. The Chairman or

nominated individual should, after seeking expert or legal advice, decide whether anyone should be notified of the breach.

7.2 Every incident should be considered on a case by case basis. The following points will help the Chairman or nominated individual to decide whether and how to notify:

7.2.1 Should the charity notify the ICO and/or affected individuals?

7.2.2 Are there any legal or contractual requirements to notify?

7.2.3 Will notification help prevent the unauthorised or unlawful use of personal data?

7.2.4 Could notification help the individual(s) affected, could they act on the information to mitigate risk?

7.2.5 How are individuals affected? This can include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised.

7.2.6 If a large number of people are affected, or there are very serious consequences, Extra Mile must notify the ICO. The ICO should only be notified if personal data is involved. There is guidance on the ICO website and helpline on when and how to notify the ICO.

7.2.7 If a breach is likely to result in a high risk to the rights and freedoms of individuals, Extra Mile must inform those concerned directly and without undue delay.

7.2.8 Consider the dangers of over-notifying. Not every incident warrants notification and overnotification may cause disproportionate investigations.

7.3 How to notify the ICO and affected individuals

7.3.1 If Extra Mile decides to notify the ICO, it must report the breach to the ICO without undue delay, but not later than 72 hours after becoming aware of the breach. If Extra Mile takes longer than that, it must give the reasons for the delay.

7.3.2 The notification should include a description of how and when the breach occurred, what data was involved and how many individuals are affected. Extra Mile should include details of what it has already done to mitigate the risks posed by the breach. Further information on what to include in a notification is to be found on the ICO's website.

7.3.3 When notifying individuals, give specific and clear advice on what they can do to protect themselves and what Extra Mile is willing to do to help them. Extra Mile should also give them the opportunity to make a formal complaint if they wish (see Extra Mile's Complaints Policy and Procedures).

7.4 If Extra Mile decides not to notify the ICO

7.4.1 If Extra Mile decides not to notify the ICO, it must still record that decision and the reasons for it.

8. Step Four: Review and Evaluation

8.1 The Chairman or nominated individual should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported in writing to the next available trustees' meeting for discussion. If systematic or ongoing problems are identified, then an action plan must be drawn up to correct the problems.

8.2 If a breach warrants a disciplinary investigation, the Chairman should take appropriate advice and guidance.

8.3 This breach policy may need to be reviewed after a breach or after legislative changes, new case law or new guidance. Consideration should be given to reviewing this breach policy whenever the Data Protection Policy is reviewed.

8.4 Advice and Assistance

8.4.1 The Chairman is responsible for data protection compliance within the charity.

8.4.2 If you have any questions or comments about the content of this policy of if you need further information, you should contact the Chairman through the charity's website: www.extra-mile.org.uk.

9. Dealing with disclosures

9.1 If an employee or other individual reports a disclosure to Extra Mile, the need for confidentiality will be respected wherever possible, although any disclosure raised under this procedure will need to be properly documented.

9.2 Extra Mile believes that all employees or other individuals should feel able to put their name to the concerns that they raise, as concerns raised anonymously are more difficult to investigate. If employees or individuals raise a concern anonymously, depending on the exact circumstances, it may still be possible for their identity to be deduced. If, contrary to this policy, they then suffer reprisals, it may be difficult to show that this was as a result of their raising a concern.

9.3 The action taken in response to a disclosure will depend on the nature of the concern. By way of example, the matters raised may result in one or more of the following:

9.3.1 no action taken;

9.3.2 action taken under other Extra Mile policies and/or procedures;

9.3.3 an internal investigation under this policy;

9.3.4 a referral to the police/ICO;

9.3.5 a referral to Extra Mile's external auditors;

9.3.6 a referral to the Charity Commission;

9.3.7 an independent enquiry.

9.4 The Chairman or other person to whom the disclosure is made will:

9.4.1 make a detailed record of the disclosure;

9.4.2 ask the employee or individual to provide a written and signed statement describing the precise nature of the concerns;

9.4.3 upon receipt of the written and signed statement, decide whether any further action may be required. If further action is required, they will refer it to the appropriate person (see

below) and write to the individual within five working days of making that decision. In their letter/ email they will acknowledge receipt of the disclosure, provide information on whom

it has been referred to and details of who the employee or individual should contact if they have any further questions.

9.5 Where further action is required under this policy in relation to the disclosure, this will typically in the first instance, take the form of an internal investigation. The internal investigator will be the Chairman, a governor of the school or a trustee of Extra Mile (as appropriate on a case by case basis). However Extra Mile may instead decide to arrange for a suitably qualified independent professional to undertake the investigation.

9.6 During the investigation the employee or individual who reported the disclosure may need to be interviewed. They will also be offered appropriate updates of progress made during the investigation, whilst bearing in mind the need to respect the confidentiality of other employees and individuals as well.

9.7 Once the investigation is complete:

9.7.1 the employee or individual will be given a prompt and thorough explanation of the result of the investigation and any action that Extra Mile is likely to take as a result of it

9.7.2 the Chairman will determine whether the disclosure is of such a nature that a report will be made to the board of trustees and/or the Charity Commission

9.7.3 any actions or recommendations that the investigator decides are required will be implemented

9.7.4 Any employee or other individual who has a genuine concern for their disclosure should feel confident in bringing forward their concerns.

9.8 Extra Mile will not tolerate any employee or other individual being subject to a detriment as a result of their making a disclosure in good faith. In the event of any employee or other individual believing that they have been subject to a detriment by anyone in Extra Mile for this reason, they must inform the Chairman immediately and appropriate action will be taken to protect them from any reprisals.

9.9 If anyone should try to discourage an employee or other individual from coming forward to express a genuine concern, Extra Mile will treat this as a disciplinary matter. In the same way, the charity will deal severely with anyone who criticises or victimise an employee or other individual or otherwise subjects them to a detriment for raising a concern.

9.10 However, if it should become clear that the procedure under this policy has not been invoked in good faith (for example, falsely or for malicious reasons or to pursue a personal grudge against another employee or other individual), this will constitute misconduct and will be treated as a disciplinary matter in accordance with Extra Mile's Disciplinary Policy.

9.11 Any employee or other individual who, in good faith, makes allegations that turn out to be unfounded will not be penalised for being genuinely mistaken.

August 2019