مؤسسة الـــروَّاد
للتعاون والتنمية
Al-Rowad Foundation
for Cooperation and Development

RCD-7-7

سياسة حماية البيانات والموافقة المستنيرة

Data Protection and Informed Consent Policy

رقم الإصدار Version No	:	V01
تاريخ الإصدار Issue Date	:	XX/XX/XXXX

تحرص مؤسسة الرواد للتعاون والتنمية على إرساء بيئة تنظيمية تقوم على مبادئ الحوكمة الرشيدة، والشفافية، والمساءلة، والكفاءة، بما يعزز من جودة الأداء المؤسسي ويضمن تحقيق الأهداف الاستراتيجية للمؤسسة.

وفي هذا السياق، تأتي هذه السياسة كجزء من مجموعة السياسات واللوائح الداخلية التي تنظم العمل في مختلف مجالات المؤسسة، وتحدد الأدوار والمسؤوليات وآليات التنفيذ والرقابة، بما يتماشى مع القيم والمبادئ الأساسية التي تتبناها المؤسسة.

تهدف هذه السياسة إلى توحيد الإجراءات والممارسات، وضمان الالتزام بالمعايير القانونية والتنظيمية والأخلاقية، مع تعزيز ثقافة العمل المؤسسي وتطوير الأداء المستدام.

تم إعداد الإصدار الأول من سياسة حماية البيانات والموافقة المستنيرة لمؤسسة الرواد للتعاون والتنمية من قبل مجلس الأمناء، وتم اعتمادها رسمياً من المدير التنفيذي للمؤسسة

1. المقدمة والهدف

تلتزم مؤسسة الرواد للتعاون والتنمية بصون كرامة المستفيدين وحماية خصوصيتهم وأمن بياناتهم الشخصية. تهدف هذه السياسة إلى تحديد الضوابط القانونية والأخلاقية لجمع، وتخزين، ومعالجة، ومشاركة البيانات التي يتم الحصول عليها أثناء الأنشطة والتقييمات الميدانية، وضمان أن تكون كل عملية جمع بيانات مبنية على موافقة حرة وعن وعي كامل من المستفيد (الموافقة المستنيرة)، تجنباً لأي استغلال أو ضرر قد يلحق بهم.

2. المبادئ الأساسية لحماية البيانات

تلتزم المؤسسة بالمبادئ الستة التالية في إدارة البيانات:

القانونية والعدالة والشفافية: جمع البيانات بطرق مشروعة وبمعرفة المستفيد الكاملة بأسباب جمعها.

تحديد الغرض: استخدام البيانات فقط للأغراض المحددة والشرعية التي أُبلغ المستفيد بها (مثل التحقق من الأهلية للمساعدات) ويُمنع استخدامها في أي سياق آخر.

الحد الأدنى من البيانات :اقتطاع وجمع البيانات الضرورية فقط للخدمة، وتجنب طرح أسئلة شخصية أو حساسة لا داعي لها.

الدقة والتحديث: الحفاظ على دقة البيانات وتحديثها وتصحيح أو حذف أي بيانات خاطئة فوراً.

تقييد التخزين :عدم الاحتفاظ بالبيانات الشخصية لفترة أطول من اللازم لتحقيق الأغراض التي جُمعت من أجلها.

النزاهة والسرية: استخدام تدابير تقنية وإدارية صارمة لحماية البيانات من الوصول غير المصرح به، أو الفقدان، أو التلف.

3. السلسلة الإجرائية لتطبيق الموافقة المستنيرة

لضمان شرعية جمع البيانات، يلتزم الباحثون الميدانيون وفريق الـ MEAL باتباع خطوات خطية صارمة للحصول على الموافقة قبل كتابة أي حرف في الاستمارة:

1. الشرح والإفصاح الكامل

قبل بدء المقابلة الميدانية

يقوم الباحث بقراءة بيان الخصوصية للمستفيد بلغة بسيطة ومفهومة، موضحاً: هوية المؤسسة، الهدف من جمع البيانات، كيفية حمايتها، والجهات التي قد تطلع عليها (كالمانحين).

2. فك الارتباط بالمساعدات

التأكيد على طوعية المشاركة

يشرح الباحث للمستفيد بوضوح شديد أن مشاركته في الاستبيان طوعية تماماً، وأن رفضه للإجابة أو لبعض الأسئلة لن يؤثر مطلقاً على حقه في تلقي المساعدات الحالية أو المستقبلية من المؤسسة.

3. الاختيار والتوثيق

تحديد نوع الموافقة

يُطلب من المستفيد تقديم موافقته؛ إما شفهياً (ويقوم الباحث بتوثيقها برقم رقمي على نظام الكوبو)، أو خطياً بالتوقيع/البصمة في الحالات الحساسة، أو عبر موافقة ولي الأمر إذا كان المستهدف طفلاً (أقل من 18 عاماً).

4. حق الانسحاب والتعديل

طوال وبعد المقابلة

إبلاغ المستفيد بأن له الحق الكامل في إنهاء المقابلة في أي وقت، أو طلب حذف بياناته وصوره من أنظمة المؤسسة حتى بعد انتهاء المقابلة، دون الحاجة لإبداء أسباب.

4. مصفوفة مستويات حساسية البيانات وضوابط حمايتها

تُصنف البيانات في مؤسسة الرواد إلى ثلاثة مستويات، ويُطبق على كل مستوى ضوابط أمنية محددة:

مستوى الحساسية	نوع البيانات المشمولة	ضوابط الحماية والوصول المعتمدة
بينات عامة	إحصائيات المشاريع الإجمالية، أعداد المستفيدين الكلية، التقارير السنوية المنشورة	متاحة للجميع على الموقع الإلكتروني ولا تحتوي على أي معلومات تدل على هوية الأفراد.
بيانات شخصية	الأسماء الكاملة، أرقام الهواتف، أرقام الهويات الشخصية، عناوين السكن، صور المستفيدين	تُشفر على السيرفر، ويُمنع تداولها في مجموعات الواتساب أو الإيميلات المفتوحة. يقتصر الوصول لمسؤول البيانات ومدير الـMEAL
بيانات حساسة	الحالة الطبية والصحية، العرق، الانتماءات، بيانات الحماية والعنف القائم على النوع الاجتماعي	يُمنع جمع الأسماء مع هذه البيانات، وتُفصل الهوية فوراً باستخدام أكواد رمزية. تخزن في سحابة مشفرة بخاصية التحقق ثنائي الخطوات

5. بروتوكول التعامل مع اختراق وحوادث البيانات

في حال حدوث أي تسريب أو وصول غير مصرح به للبيانات (مثل فقدان هاتف/جهاز لوحي يحتوي على استمارات، أو اختراق حساب السيرفر)، تلتزم المؤسسة بالخطوات التالية:

1. الاحتواء الفوري (في أول 24 ساعة): يقوم قسم تكنولوجيا المعلومات (IT) بالتعاون مع الـ MEAL بتجميد الحسابات المخترقة، وتغيير كلمات المرور، ومسح البيانات عن الأجهزة المفقودة عن بعد.

2. تقييم المخاطر: تحديد حجم البيانات المسربة ومدى خطورتها على أمن وسلامة المستفيدين ميدانياً.

3. الإخطار والشفافية (في أول 72 ساعة): تلتزم المؤسسة بإبلاغ المانح المتضرر، وإذا كان التسريب يشكل خطراً وثيقاً على المستفيدين، يتم إعلامهم بالتعاون مع اللجان المجتمعية لاتخاذ الاحتياطات الأمنية اللازمة.

6. الالتزام وبناء القدرات

- يُوقع كافة موظفي قسم الـMEAL ، مدخلي البيانات، والجامعين الميدانيين (اليوميين) على اتفاقية الحفاظ على سرية البيانات وعدم الإفصاح كجزء أساسي من عقودهم.
- يُحظر تماماً على الموظفين استخدام هواتفهم الشخصية لتصوير المستفيدين أو وثائقهم، ويتم الاعتماد حصراً على أجهزة المؤسسة المصرحة.
- يخضع فريق العمل لتدريب دوري حول الأمن السيبراني وأخلاقيات التعامل مع البيانات الشخصية.

ملاحظة: يعتبر الامتثال لهذه السياسة إلزامياً، وأي مخالفة لبنودها (مثل مشاركة قوائم المستفيدين مع جهات خارجية دون إذن رسمي، أو تصوير المستفيدين دون موافقة مستنيرة) تعرّض الموظف للمساءلة القانونية والفصل الفوري بتهمة خرق مدونة السلوك وسياسة الحماية.