MISY | Mandalay
Myanmar International School Yangon (Mandalay Campus)

Myanmar International School Yangon

(MANDALAY CAMPUS)

သတင်းအချက်အလက်ကာကွယ်ရေး မူဝါဒ

Approved by:	Nu Nu Aye (BOD)	**Date:** July 23, 2023
Last reviewed on:	October 2025	
Next review due by:	October 2027	

WIDA INTERNATIONAL SCHOOL CONSORTIUM MEMBER SCHOOL

CAMBRIDGE International Education
Cambridge International School

ဝေါဟာရများ ။

အချက်အလက်ကာကွယ်မှု : အရေးကြီးသော အချက်အလက်များကို အဂတိလိုက်စားမှု၊ အပေးအယူပြုလုပ်ခံရမှု သို့မဟုတ် ဆုံးရှုံးမှုများမှ ကာကွယ်ပေးသောလုပ်ငန်းစဉ်ဖြစ်ပါသည်။

ကိုယ်ရေးကိုယ်တာ အချက်အလက်: လူပုဂ္ဂိုလ်တစ်ဦးတစ်ယောက်အား ကိုယ်စားပြု သက်ဆိုင်သည့် မည်သည့်အချက်အလက်မဆို သို့မဟုတ် လူပုဂ္ဂိုလ်တစ်ယောက်အား ဖော်ထုတ်နိုင်သော မည်သည့် အချက်အလက်မဆိုသည် ကိုယ်ရေးကိုယ်တာ အချက်အလက်များဖြစ်ပါသည်။ ဥပမာ- ဖုန်းနံပါတ်၊ အကြွေးဝယ်ကဒ်နံပါတ် သို့မဟုတ် လူတစ်ယောက်၏ကိုယ်ပိုင်နံပါတ်များဖြစ်သော ဝန်ထမ်းနံပါတ်၊ အကောင့်ဒေတာ၊ နံပါတ်ပြား၊ အသွင်အပြင်၊ ဖောက်သည်နံပါတ် သို့မဟုတ် လိပ်စာအားလုံးသည် ကိုယ်ရေးကိုယ်တာအချက်အလက်များဖြစ်သည်။

အချက်အလက်ပိုင်ရှင်များ (Data Subjects): ကိုယ်ရေးကိုယ်တာအချက်အလက်ပိုင်ရှင်များ (မိဘများ၊ ကျောင်းသားများ စသည်ဖြင့်)။

အချက်အလက်များကို ထိန်းသိန်းသူ (Data controller): Myanmar International School of Yangon (Mandalay)

အချက်အလက်စီမံဆောင်ရွက်သူ(Data processor): အချက်အလက်များကို လုပ်ဆောင်ရန် တာဝန်ရှိသူ။

အချက်အလက်စီမံခန့်ခွဲမှုတာဝန်ခံများ(Data stewards): ကျောင်း၏မတူညီသောနယ်ပယ်များမှ ကိုယ်ရေး ကိုယ်တာ အချက်အလက်များကို စီမံဆောင်ရွက်သည့် နည်းလမ်းများကို ဆုံးဖြတ်ရန် ရည်ရွယ်ချက်ဖြင့် တာဝန် ပေးအပ်ထားသော ဝန်ထမ်းအဖွဲ့ဝင်များ။

ကိုယ်ရေးကိုယ်တာအချက်အလက်သတိပေးစာ: ၎င်းတို့၏ ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို မည်သို့ လုပ်ဆောင်နေသည်ဟူသော ရည်ရွယ်ချက်အတွက် ၎င်းတို့အား အသိပေးရန် အချက်အလက်ပိုင်ရှင်အား စာဖြင့်ဆက်သွယ်ခြင်း။

Introduction

Myanmar International School Yangon (MISY) သည် ပြည်ထောင်စု သမ္မတ မြန်မာနိုင်ငံတော်တွင် အချက်အလက် ကာကွယ်ရေးနှင့် စပ်လျဉ်းသည့် ဥပဒေများနှင့် စည်းမျဉ်း လမ်းညွှန်မှုများအောက်တွင် တည်ရှိပါသည်။ ထို့အပြင်၊ MISY သည် သက်ဆိုင်ရာ ပြည်တွင်းနှင့် နိုင်ငံတကာ ဆိုင်ရာ တာဝန်များကို ဖြည့်ဆည်းပေးနိုင်သည့် ကျွန်ုပ်တို့၏ မူဝါဒများနှင့် လုပ်ထုံးလုပ်နည်းများအတိုင်း ကိုက်ညီမှုရှိစေရန် ကျွန်ုပ်တို့၏အချက်အလက်ကာကွယ်ရေးကို ဖွဲ့စည်းတည်ဆောက်ထားပါသည်။

MISY သည် ဝန်ထမ်းများ၊ ကျောင်းသားများ၊ မိဘများ၊ ဧည့်သည်များနှင့် ကျောင်းသားဟောင်းများ အပါအဝင်၊ အလုပ်လုပ်ကိုင်နေသူအားလုံး၏ အချက်အလက်ကာကွယ်ရေးအခွင့်အရေးများကို ပံ့ပိုးပေးပါသည်။ ဤမူဝါဒသည် မူဝါဒပါ ပြဋ္ဌာန်းချက်များကို အတတ်နိုင်ဆုံး လိုက်နာရန် ကျောင်း၊ ၎င်း၏ ဝန်ထမ်းများနှင့် ၎င်း၏ ကျောင်းသားကျောင်းသူများ၏ တာဝန်ခံမှုနှင့် တာဝန်များကို ပြဋ္ဌာန်းထားသည်။ MISY သည် “Data Subject”ဟု သတ်မှတ်ထားသော ဝန်ထမ်းများ၊ ကျောင်းသား ကျောင်းသူများ၊ ဘွဲ့ရများနှင့် အခြားသူများကဲ့သို့သော ပုဂ္ဂိုလ်ရေးဆိုင်ရာ ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို သိမ်းဆည်းပြီး စီမံဆောင်ရွက်ပါသည်။

မူဝါဒ၏ရည်ရွယ်ချက်

ဤမူဝါဒတွင် ပြည်ထောင်စုသမ္မတ မြန်မာနိုင်ငံတော်အတွင်း ရှိ အချက်အလက် ကာကွယ်ရေးနှင့် ပတ်သတ်သည့် ဥပဒေများနှင့် သက်ဆိုင်ရာပြည်တွင်းနှင့် နိုင်ငံတကာလုပ်ထုံးလုပ်နည်းများနှင့် MISY ၏အတွင်းရေးရာမူဝါဒများနှင့် နည်းလမ်းများအတိုင်းလိုက်နာနိုင်ရန်အတွက် ကျောင်း၊ ဦးစီးအဖွဲ့ဝင်များ၊ မိဘများ၊ ဝန်ထမ်းများနှင့် ကျောင်းသား ကျောင်းသူ များ၏တာဝန်ဝတ္တရားများကို ဖော်ပြထားပါသည်။

မူဝါဒနှင့်တွဲဖက်၍ MISY ၏အထူးဌာနများအတွက် အချက်အလက်ကာကွယ်ရေး၏ အမျိုးမျိုးသော အခြေအနေများနှင့် လမ်းညွှန်ချက်များကို ဖော်ပြသော အချက်အလက်ကာကွယ်ရေး လက်စွဲစာအုပ် တစ်အုပ်လည်း ပါဝင်ပါသည်။

ဤမူဝါဒနှင့် လက်စွဲစာအုပ်သည် ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို ကိုင်တွယ်လုပ်ဆောင်သော လူတိုင်းအတွက်လိုက်နာရန်လိုအပ်သော မူဝါဒအခြေခံအစီအစဉ်တစ်ရပ်ဖြစ်ပါသည်။

မူဝါဒ၏လွှမ်းမိုးမှုအတိုင်းအတာ

ဤမူဝါဒသည် MISY (မန္တလေး) သည် ကိုယ်ရေးကိုယ်တာအချက်အလက်များအတွက် အချက်အလက်ထိန်းချုပ်သူ (Data Controller) သို့မဟုတ် အချက်အလက်ကိုင်တွယ်သူ (Data Processor) ဖြစ်သော အခြေအနေများတွင် ဘုတ်အဖွဲ့ဝင်များ၊ မိဘများ၊ ဝန်ထမ်းများနှင့် ကျောင်းသား ကျောင်းသူများအားလုံးအတွက် သက်ဆိုင်မည့် မူဝါဒဖြစ်ပါသည်။

အချက်အလက်ကို မည်သူက ဖန်တီးသည်၊ မည်သည့်နေရာတွင် ထိန်းသိမ်းထားသည် သို့မဟုတ် အသုံးပြုသည့် ပစ္စည်းများ၏ ပိုင်ဆိုင်မှုကို မခွဲခြားဘဲ ဤကိစ္စရပ်များတွင် မူဝါဒသည် အကျုံးဝင်ပါသည်။

မူဝါဒအချက်အလက်များ

ဤမူဝါဒသည် ဝန်ထမ်းများအားလုံးအတွက် မဖြစ်မနေလိုက်နာရမည့်အခြေအနေတစ်ခုဖြစ်ပြီး ဘုတ်အဖွဲ့ဝင်များ၊ မိဘများနှင့် ကျောင်းသားများအားလုံးသည်လည်း ကျောင်း၏မူဝါဒနှင့် လုပ်ထုံးလုပ်နည်းများကို လိုက်နာရန်မျှော်လင့်ပါသည်။ ကျောင်းနှင့်လက်တွဲလုပ်ဆောင်နေသော ကျောင်းကန်ထရိုက်တာများနှင့် ပြင်ပအဖွဲ့အစည်းများသည်လည်း ဤစံနှုန်းများကို လိုက်နာရန် တောင်းဆိုသွားမည်ဖြစ်ပါသည်။

တာဝန်များ

ဒါရိုက်တာဘုတ်အဖွဲ့ (BOD) သည် ပြန်လည် စစ်ဆေးသည့်အခါတိုင်း အတည်ပြုမည်ဖြစ်ပြီး၊ မူဝါဒသည် ဥပဒေနှင့် ကိုက်ညီမှုရှိကြောင်းသေချာစေပြီး၊ မူဝါဒ အကောင်အထည်ဖော်ဆောင်ရွက်မှုအတွက် ကျောင်းအုပ်ကြီးကို တာဝန်ခံအဖြစ်ထမ်းဆောင်စေမည်ဖြစ်သည်။

ဒါရိုက်တာဘုတ်အဖွဲ့သည် ဤမူဝါဒ၏ ထိရောက်မှုကို စောင့်ကြည့်ထိန်းချုပ်ရန်အတွက် ဒါရိုက်တာဘုတ်အဖွဲ့ဝင်တစ်ဦးကို တာဝန်ပေးအပ်မည်ဖြစ်သည်။

ဒါရိုက်တာဘုတ်အဖွဲ့သည် ဤဒေတာထိန်းသိမ်းရေးမူဝါဒနှင့်ဆက်နွယ်သည့် အခြားစာရွက်စာတမ်းများ အပေါ်တွင် ကျောင်းအုပ်ကြီးမှ အတည်ပြုပေးထားသည့်အတိုင်း ဝင်ရောက်ကြည့်ရှုခွင့်ရှိမည်ဖြစ်သည်။

အရေးပေါ်အခြေအနေများ၊ ခွင့်ပြုချက်ချိုးဖောက်မှုများ၊ ETC Co., Ltd ကိုယ်စားပြု ဆောင်ရွက်ရသည့် ဥပဒေကြောင်းအရအခြေအနေများ တွင် ဒါရိုက်တာဘုတ်အဖွဲ့သည် ဒေတာကို ကိုင်တွယ် ဆောင်ရွက်ရာတွင် နောက်ဆုံး အခွင့်အာဏာကို ရရှိမည်ဖြစ်သည်။

ဒေတာထိန်းသိမ်းရေးအရာရှိ(The Data Protection Officer)သည် ဒေတာကို ဆက်လက်ကိုင်တွယ်ဆောင်ရွက်ရန် တာဝန်ရှိသော ဝန်ထမ်းများအားလုံးသည် ဤမူဝါဒနှင့် လုပ်ထုံးလုပ်နည်းများကို နားလည်သဘောပေါက်စေရန် ဆောင်ရွက်မည်ဖြစ်ပြီး၊ မူဝါဒနှင့်ပတ်သက်သော လေ့ကျင့်သင်ကြားမှုများကို ဝန်ထမ်းများအားလုံးအတွက် လုံလောက်အောင် ပေးအပ်မည်ဖြစ်သည်။ ထို့အပြင် မူဝါဒကို နေ့စဉ်အကောင်အထည်ဖော်ဆောင်ရွက်ရာတွင် ဖြစ်ပေါ်လာသောအရာများအားလုံးအပေါ်တွင် ကျောင်းအုပ်၊ ဒါရိုက်တာဘုတ်အဖွဲ့တို့နှင့် ပေါင်းစည်းညှိနှိုင်းဆောင်ရွက်မည်ဖြစ်သည်။

ကျောင်းအုပ်နှင့် ဒေတာစီမံခန့်ခွဲမှုအတွက် တာဝန်ရှိသော ဝန်ထမ်းများအားလုံးသည် ဤမူဝါဒနှင့် ကိုက်ညီသည့်နည်းလမ်းဖြင့် လိုက်နာဆောင်ရွက်ကြောင်းသေချာစေရန် တာဝန်ရှိသလို၊ မိမိတို့တာဝန်ယူသောဧရိယာအတွင်း သတင်းအချက်အလက်ကို ကောင်းမွန်စွာ ကိုင်တွယ်ဆောင်ရွက်သည့် အလေ့အထ များ ရှိစေရန် တိုက်တွန်း ဖော်ဆောင်ရမည်ဖြစ်သည်။ ကျောင်းအတွင်းရှိ ကိုယ်ပိုင်ဒေတာအသုံးပြုသူအားလုံးသည် ဤမူဝါဒတွင် ဖော်ပြထားသော အခြေခံသတ်မှတ်ချက်များနှင့် လိုက်နာရန်လိုအပ်သော အခြားအချက်အလက်များအတိုင်း ဒေတာကို ကိုင်တွယ်ဆောင်ရွက်ကြောင်း သေချာစေရန် တာဝန်ရှိသည်။ ဒေတာထိန်းသိမ်းရေး လက်စွဲစာအုပ်သည် ဤတာဝန်များကို ပြည့်မှီအောင် ဆောင်ရွက်နိုင်ရန်အတွက် အသေးစိတ်ညွှန်ကြားချက်များ ပေးထားပါသည်။

အချက်အလက်လုံခြုံရေး

ကျောင်းအတွင်းရှိ ကိုယ်ရေးကိုယ်တာဒေတာအသုံးပြုသူအားလုံးသည် ကိုယ်ရေးကိုယ်တာ အချက်အလက်များကို အမြဲလုံခြုံစွာ ထိန်းသိမ်းထားရန်နှင့် မတော်တဆ၊ ပေါ့ပေါ့ဆဆ သို့မဟုတ် ရည်ရွယ်ချက်ရှိရှိ သို့မဟုတ် ခွင့်ပြုချက်မရှိဘဲ မည်သည့်ပြင်ပအဖွဲ့အစည်းကိုမျှ ထုတ်ဖော်မပေးအပ်ကြောင်း သေချာစေရမည်။

ကိုယ်ရေးကိုယ်တာ သတိပေးချက်များ

ကျောင်းသည် တစ်ဦးချင်းစီထံမှ ကိုယ်ရေးကိုယ်တာ အချက်အလက်များကို စုဆောင်းသည့်အခါ 'တရားမျှတမှုနှင့် ပွင့်လင်းမြင်သာမှု' အတွက် လိုအပ်ချက်ကို လိုက်နာရမည်ဖြစ်သည်။ ဆိုလိုသည်မှာ ကျောင်းသည် ၎င်းတို့၏ ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို မည်သို့လုပ်ဆောင်ပြီး မည်သည့် ရည်ရွယ်ချက်ဖြင့် လုပ်ဆောင်သည်ကို သိရှိစေရန် 'ကိုယ်ရေးကိုယ်တာသတိပေးချက်' ဖြင့် အချက်အလက်ပိုင်ရှင်များ (Data Subjects) ကို အသိပေးရမည်ဖြစ်သည်။ ဒေတာလုပ်ဆောင်ခြင်း မှန်သမျှသည် ထိုရည်ရွယ်ချက်နှင့် တသမတ်တည်းဖြစ်ရမည်။

လုပ်ဆောင်မှုအခြေအနေများ

ဤမူဝါဒ၏ လိုအပ်ချက်များနှင့် ကိုက်ညီစေရန်၊ ကိုယ်ရေးကိုယ်တာအချက်အလက်ကို စီမံဆောင်ရွက်ရာတွင် အောက်ပါအခြေအနေများအနက်မှ အနည်းဆုံးတစ်ခုနှင့် ကိုက်ညီရမည်-

၁။ အချက်အလက်ပိုင်ရှင်များ (Data Subjects)မှ သဘောတူညီမှုပေးသည်။

၂။ စာချုပ်ပါအချက်အရ စီမံဆောင်ရွက်ပေးရန် လိုအပ်ခြင်း။

၃။ ဥပဒေပါ တာဝန်ကြောင့် လိုအပ်ပါသည်။

၄။ တစ်စုံတစ်ယောက်၏ အရေးကြီးသော အကျိုးစီးပွားများ (ဆိုလိုသည်မှာ အသက် သို့မဟုတ် သေဆုံးမှု အခြေအနေ) ကို ကာကွယ်ရန် လိုအပ်ခြင်း။

၅။ အများသူငှာ အကျိုးစီးပွားအတွက် ဆောင်ရွက်သည့်တာဝန်တစ်ရပ်ကို ပြည့်စုံအောင် ဆောင်ရွက်ရန် သို့မဟုတ် ထိန်းချုပ်သူအား တရားဝင်အပ်နှင်းထားသော အခွင့်အာဏာကို ကျင့်သုံးရန်အတွက် လိုအပ်ခြင်း။

၆။ ထိန်းချုပ်သူ သို့မဟုတ် ပြင်ပအဖွဲ့အစည်း၏ တရားဝင် အကျိုးစီးပွားအတွက် လိုအပ်ခြင်း။

ပုဂ္ဂိုလ်ရေးဒေတာအထူးအမျိုးအစားများအတွက် ကိုယ်ရေးကိုယ်တာအချက်အလက်များအား အသုံးပြုရန် အနည်းဆုံး အောက်ပါအခြေအနေများထဲမှ တစ်ခုဖြစ်ပေါ်ရမည်ရမည် -

၁။ အချက်အလက်ပိုင်ရှင်များ (Data Subjects) မှ အချက်အလက်အကြောင်းအရာအားအသုံးပြုရန် ပြတ်သားစွာ သဘောတူခွင့်ပြုခြင်း။

၂။ အလုပ်အကိုင်ဆိုင်ရာနှင့် ဒေသန္တရအစိုးရ လိုအပ်ချက်များအတွက် အသုံးပြုရန်လိုအပ်ခြင်း။

၃။ တစ်စုံတစ်ဦး၏ အရေးပါသော အကျိုးစီးပွားများကို ကာကွယ်ရန် စီမံဆောင်ရွက်မှုများ လိုအပ်ခြင်း။

၄။ အဆိုပါဒေတာ သည် အကျိုးအမြတ်မယူသော အဖွဲ့အစည်း အတွက်အသုံးပြုခြင်း။

၅။ စီမံဆောင်ရွက်ခြင်းကို အချက်အလက်ပိုင်ရှင်များ (Data Subjects) မှ အများသိအောင် ထင်ရှားစွာပြသခြင်း။

၆။ ဥပဒေကြောင်းအရ တောင်းဆိုမှုများအတွက် စီမံဆောင်ရွက်ပေးရန် လိုအပ်ခြင်း။

၇။ အများသူငှာ အကျိုးစီးပွားအတွက် စီမံဆောင်ရွက်ပေးရန် လိုအပ်ခြင်း။

၈။ ဆေးဝါးကုသမှုဆိုင်ရာ ရည်ရွယ်ချက်များ၊ ကျန်းမာရေး သို့မဟုတ် လူမှုရေးစောင့်ရှောက်မှု သို့မဟုတ် ကုသမှု သို့မဟုတ် ကျန်းမာရေးစီမံခန့်ခွဲမှု သို့မဟုတ် လူမှုရေးစောင့်ရှောက်မှုစနစ်များနှင့် ဝန်ဆောင်မှုများကို ဆောင်ရွက်ရန်အတွက် လိုအပ်ခြင်း။

၉။ ပြည်သူ့ကျန်းမာရေးအတွက် စီမံဆောင်ရွက်ပေးရန် လိုအပ်ပါသည်။

၁၀။ လက်စွဲစာအုပ်တွင် ရှင်းပြထားသည့် အချို့သော လုံခြုံရေးအကာအကွယ်များ အရ အများအကျိုး၊ သိပ္ပံနည်းကျ သို့မဟုတ် သမိုင်းဆိုင်ရာ သုတေသန ရည်ရွယ်ချက်များ သို့မဟုတ် စာရင်းအင်းဆိုင်ရာ ရည်ရွယ်ချက်များအတွက် သိမ်းဆည်းခြင်း အသုံးပြုခြင်း။

အချက်အလက်ထိန်းသိမ်းမှု

မူလသိမ်းဆည်းခြင်း၏ ရည်ရွယ်ချက်များအတွက် ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို လိုအပ်သည်ထက် ပိုကြာအောင် မသိမ်းဆည်းရပါ။ ဤအချက်သည် ပင်မစနစ်များ၊ ဒေသခံ PC များ၊ လက်ပ်တော့များ သို့မဟုတ် မိုဘိုင်းလ်စက်ပစ္စည်းများ သို့မဟုတ် စာရွက်ပေါ်တွင် သိမ်းဆည်းထားသည်ဖြစ်စေ ကိုယ်ရေးကိုယ်တာ အချက်အလက်အားလုံးနှင့် သက်ဆိုင်ပါသည်။ အချက်အလက်များ မလိုအပ်တော့ပါက ယင်းတို့ကို လုံခြုံစွာ ဖျက်သိမ်းရန် သို့မဟုတ် ဖျက်ပစ်ရန် လုပ်ဆောင်ရမည် ဖြစ်သည်။

ဒေတာသိမ်းဆည်းမှု လမ်းညွှန်ချက်များမှာ အောက်ပါအတိုင်း ဖြစ်ပါသည်။

- ထွက်သွားသောဝန်ထမ်း : ၁၀ နှစ်
- ထွက်သွားသော ကျောင်းသား : ၁၀နှစ် ၊ အများဆုံး ၁၅ နှစ်
- အလုပ်လျှောက်လွှာများနှင့် ကျောင်းလျှောက်လွှာများ (မပြီးစီးသေးသော၊ ရွေးချယ်မှုမရရှိသောသူများ အတွက်): ၃ နှစ်

ပုံသေသတ်မှတ်ချက်အတိုင်း ကာကွယ်ခြင်း

MISY တွင် ဆောင်ရွက်သည့် လုပ်ငန်းစဉ်အားလုံးတွင် ပုဂ္ဂိုလ်ရေးအချက်အလက် လုံခြုံရေးအပေါ် သက်ရောက်မှုကို စဉ်းစားရန် တာဝန်ရှိသည်။ ၎င်းတွင် အချက်အလက်ပိုင်ရှင်များ၏ ပုဂ္ဂိုလ်ရေးကို ထိခိုက်နိုင်သည့် ဖြစ်နိုင်ခြေများကို အနည်းဆုံးအထိ လျှော့ချနိုင်ရန်အတွက် သင့်လျော်သော နည်းပညာပိုင်းဆိုင်ရာ နှင့် အဖွဲ့အစည်းဆိုင်ရာ လုပ်ထုံးလုပ်နည်းများကို အသုံးချခြင်းပါဝင်သည်။

အချက်အလက် ကာကွယ်ရေး သက်ရောက်မှုခန့်မှန်းခြင်း

လုပ်ဆောင်မှုအသစ်များကို ထည့်သွင်းစဉ်းစားသည့်အခါ သို့မဟုတ် ကိုယ်ရေးကိုယ်တာအချက်အလက် ကိုယ်ရေးကိုယ်တာပြဿနာများပါဝင်သည့် လုပ်ထုံးလုပ်နည်းအသစ်များ သို့မဟုတ် စနစ်များ ထည့်သွင်းသည့်အခါတွင် အစောဆုံးအဆင့်မှစ၍ ဤပြဿနာများကို စဉ်းစားသုံးသပ်သင့်ပါသည်။ ၎င်းသည် လုပ်ငန်းစဉ်ဒီဇိုင်းအဆင့်များနှင့် စီမံချက်၏ ဖြစ်စဉ်စက်ဝန်းအဆင့်များ တစ်လျှောက်လုံးတွင် ဖြစ်နိုင်သည့် အန္တရာယ်များကို လျော့ချရန် အထောက်အကူဖြစ်စေပါသည်။

အမည်ဝှက်ခြင်းနှင့် စကားဝှက်ကုတ်အသုံးပြုခြင်း

ကိုယ်ရေးကိုယ်တာ အချက်အလက်များကို ကိုင်တွယ်ခြင်းနှင့် ဆက်စပ်သော အန္တရာယ်များကို လျှော့ချခြင်း၏ နောက်ထပ် ယန္တရားများမှာ အမည်ဝှက်ခြင်း သို့မဟုတ် စကားဝှက်ကုတ်အသုံးပြုခြင်း ဖြစ်သည်။ လိုအပ်သည့်အခါတိုင်း ပုဂ္ဂိုလ်ရေးအချက်အလက်များကို အမည်ဝှက်ရမည် (anonymise)၊ မဖြစ်နိုင်ပါက စကားဝှက်ကုဒ်သတ်မှတ်ရမည် (pseudonymise)။

သုတေသနပြုထားသော ဒေတာများကိုကိုင်တွယ်ခြင်း

ကိုယ်ရေးကိုယ်တာအချက်အလက်နှင့် ကိုယ်ရေးကိုယ်တာအချက်အလက်များ၏ အထူးအမျိုးအစားများကို ရယူခြင်း သို့မဟုတ် အသုံးပြုခြင်းတို့ပါဝင်မည့် မည်သည့်သုတေသနကိုမဆို

စတင်ခြင်းမပြုမီ၊ သုတေသီသည် ဤမူဝါဒနှင့် အချက်အလက်ကာကွယ်ရေးလက်စွဲစာအုပ်ပါရှိသော လမ်းညွှန်ချက်တို့ကို သင့်လျော်စွာ ထည့်သွင်းစဉ်းစားရပါမည်။ သုတေသီသည် တရားမျှတမှုနှင့် ပွင့်လင်းမြင်သာမှုကို လိုက်နာကြောင်းနှင့် သီးသန့်တည်ရှိမှုကို ပုံစံချထားသည့်အတိုင်းနှင့် ပုံသေပုံသေအတိုင်း ကျင့်သုံးကြောင်း သေချာစေရမည်။ ဆိုလိုသည်မှာ ဖြစ်နိုင်သည့်နေရာတိုင်းတွင် သုတေသနအချက်အလက်များကို ဖြစ်နိုင်ခြေအစောဆုံးအချိန်၌ အမည်ဝှက်ခြင်း နှင့် နာမည်ဝှက်ကုတ်အသုံးပြုခြင်းကို ပြုလုပ်ရမည်ဖြစ်သည်။

ကျောင်းသားကျောင်းသူများမှ ကိုယ်ရေးကိုယ်တာ အချက်အလက်များကို ကိုင်တွယ်ခြင်း။
ကျောင်းသားကျောင်းသူများက ပုဂ္ဂိုလ်ရေးအချက်အလက်များကို အသုံးပြုခြင်းသည် အောက်ဖော်ပြပါ အချက်များအရ စည်းမျဉ်းစည်းကမ်းဖြင့် ထိန်းသိမ်းထားသည် -

- ကျောင်းသားကျောင်းသူတစ်ဦးသည် မိမိလေ့လာသင်ကြားမှုအတွက် ပုဂ္ဂိုလ်ရေးအချက်အလက်များကို စုဆောင်းပြီး စီမံဆောင်ရွက်သည့်အခါ၊ ထိုလေ့လာမှုသည် ကျောင်းမှဦးဆောင်သည့် ပရောဂျက်တစ်ခု မဟုတ်ပါက၊ ကျောင်းသားကျောင်းသူသည် သုတေသနတွင် အသုံးပြုသည့် ကိုယ်ရေးကိုယ်တာ အချက်အလက်များအတွက် အချက်အလက်ထိန်းချုပ်သူမဟုတ်ဘဲ ကျောင်းသည်သာ အချက်အလက် ထိန်းချုပ်သူဖြစ်သည်။ အချက်အလက်များကို ကျောင်းက ကိုင်ဆောင်ထားပြီးဖြစ်သော ဒေတာဘေ့စ်မှ ထုတ်ယူပါက၊ ကျောင်းသည် ဒေတာဘေ့စ်အတွက် အချက်အလက်ထိန်းချုပ်သူအဖြစ် ကျန်ရှိနေသော်လည်း ကျောင်းသား ကျောင်းသူသည် ထုတ်ယူထားသောဒေတာအတွက် အချက်အလက် ထိန်းချုပ်သူ ဖြစ်လာမည်ဖြစ်သည်။
- ပုဂ္ဂိုလ်ရေးအချက်အလက်များ ပါဝင်သည့် ဆောင်ရွက်ချက်တစ်ခုကို စစ်ဆေးမှုအတွက် တင်သွင်းသောအခါမှစ၍၊ ထိုပုဂ္ဂိုလ်ရေးအချက်အလက်များအတွက် ကျောင်းက အချက်အလက် ထိန်းချုပ်သူ ဖြစ်လာသည်။
- ဝန်ထမ်းတစ်ဦးမှ ဦးဆောင်သည့် ပရောဂျက်တစ်ခုတွင် လုပ်ဆောင်နေစဉ် သုတေသနကျောင်းသား ကျောင်းသူသည် ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို စီမံဆောင်ရွက်သည့်အခါတွင် ကျောင်းသည် အချက်အလက်ထိန်းချုပ်သူဖြစ်သည်။

ဝန်ထမ်းအားလုံးသည် ၎င်းတို့ကြီးကြပ်သည့် ကျောင်းသား ကျောင်းသူများအား အောက်ပါတို့ကို သိရှိကြောင်း သေချာစေရမည် -

- ကျောင်းသားတစ်ဦးသည် ကျောင်းနှင့်ဆက်စပ်သည့်ရည်ရွယ်ချက်အတွက် ပုဂ္ဂိုလ်ရေးအချက်အလက်များကို အသုံးပြုရန်ဆိုပါက၊ သင့်လျော်သောဝန်ထမ်းတစ်ဦး၏ အသိအမှတ်ပြုမှုနှင့် တိကျကြောင်းပြသသည့် ခွင့်ပြုချက် ရရှိပြီးမှသာ အသုံးပြုသင့်သည်။
- ကျောင်းသား ကျောင်းသူများသည် ကျောင်းနှင့်ဆက်နွယ်သော ပုဂ္ဂိုလ်ရေးအချက်အလက်များကို အသုံးပြုရာတွင်၊ ပညာရေးဆိုင်ရာ ရည်မှန်းချက်များ ပြည့်မီစေရန်အတွက် အနည်းဆုံး လိုအပ်သည့်အတိုင်းသာ အသုံးပြုသင့်သည်။ ကျောင်းသား ကျောင်းသူများက ဒေတာပိုင်ရှင်ကို မဖော်ထုတ်နိုင်စေရန် ဖြစ်နိုင်သမျှ ဒေတာများကို အမည်မသိအောင် (anonymise) ပြုလုပ်ရန် လိုအပ်ပါသည်။

အချက်အလက် ပိုင်ရှင်များ၏ အခွင့်အရေးများ

အချက်အလက် ဝင်ရောက်ခွင့်တောင်းဆိုမှုများနှင့် ဒေတာပြောင်းရွှေ့မှုအခွင့်အရေး

တစ်ဦးချင်းစီသည် ၎င်းတို့နှင့်ပတ်သက်သည့် ကျောင်းမှရရှိထားသော အချက်အလက်များ၏ မိတ္တူများကို ကြည့်ရှုရန် သို့မဟုတ် လက်ခံရယူရန် တောင်းဆိုပိုင်ခွင့်ရှိပြီး အချို့အခြေအနေများတွင် အဆိုပါ အချက်အလက်များကို စနစ်တကျ၊ အသုံးများပြီး စက်ဖြင့်ဖတ်နိုင်သော ဖော်မတ်ဖြင့် အခြားအချက်အလက် ထိန်းချုပ်ကိရိယာသို့ ထပ်ဆင့်ပေးပို့နိုင်စေရန် တောင်းဆိုပိုင်ခွင့်ရှိသည်။ ကျောင်းသည် ဤတောင်းဆိုချက်များကို လေးပတ်အတွင်း တုံ့ပြန်ရမည်။ ဝင်ရောက်ခွင့်တောင်းဆိုချက်ကို မဖြည့်ဆည်းမီ တောင်းဆိုထားသော ကိုယ်ရေးကိုယ်တာအချက်အလက်ကို ဖျက်ပစ်ခြင်းကို ကန့်သတ်ထားရမည်။

ဖျက်ပိုင်ခွင့် လုပ်ဆောင်ခြင်းကို ကန့်သတ်ခွင့်၊ဖြည့်စွက်ပြင်ဆင်ခွင့် နှင့် ကန့်ကွက်ပိုင်ခွင့်

အချို့သောအခြေအနေများတွင် ဒေတာအကြောင်းအရာများသည် ၎င်းတို့၏ဒေတာများကို ဖျက်ပိုင်ခွင့်ရှိသည်။ ၎င်းသည် အောက်ပါအခြေအနေများတွင် အကျုံးဝင်သည်-

- အချက်အလက် ကို မူလရည်ရွယ်ချက်အတွက် ထပ်မံ မလိုအပ်တော့သည့်အခါ။
- Data subject (အချက်အလက်ပိုင်ရှင်) မှ ခွင့်ပြုချက်ကို ရုပ်သိမ်းသည့်အခါ။
- အချက်အလက်များကို ဥပဒေမဲ့ လုပ်ဆောင်သည့်အခါ။

အချို့သောအခြေအနေများတွင်၊ Data subject သည် ၎င်းတို့၏အချက်အလက်ကို ဖျက်ပစ်ရန် ဆန္ဒမရှိသော်လည်း နောက်ထပ်လုပ်ဆောင်မှုအား ကန့်သတ်ခွင့်ရှိသည်။

ပုဂ္ဂိုလ်ရေးအချက်အလက်များမှာ မှားယွင်းနေပါက၊ ဒေတာပိုင်ရှင်သည် ကျောင်းထံမှ ထိုအချက်အလက်များကို ပြင်ဆင်ပေးရန် တောင်းဆိုခွင့်ရှိသည်။ အချို့သောအခြေအနေများတွင်၊ ပုဂ္ဂိုလ်ရေးအချက်အလက်များ မပြီးစီးဘဲ မဖြည့်စွက်ဘဲ ရှိနေပါက၊ ဒေတာပိုင်ရှင်သည် ဒေတာထိန်းချုပ်သူထံမှ ထိုအချက်အလက်များကို ဖြည့်စွက်ရန် သို့မဟုတ် ဖြည့်စွက်ရှင်းလင်းချက်တစ်ရပ် ထည့်သွင်းဖော်ပြရန် တောင်းဆိုခွင့်ရှိသည်။

Data subject သည် တိုက်ရိုက်ဈေးကွက်ရှာဖွေရေး၊ သုတေသန သို့မဟုတ် စာရင်းအင်းဆိုင်ရာ ရည်ရွယ်ချက်များအတွက် လုပ်ဆောင်ခြင်းကဲ့သို့သော သီးခြားလုပ်ဆောင်မှုအမျိုးအစားများကို ကန့်ကွက်ပိုင်ခွင့်ရှိသည်။ Data subject သည် ကိုယ်ပိုင်အခြေအနေနှင့် သက်ဆိုင်သည့် ဒေတာဆောင်ရွက်ခြင်း အား ကန့်ကွက်လိုကြောင်း အခြေခံအကြောင်းတရားများကို ဖော်ပြရန် လိုအပ်ပါသည်။ သို့သော် တိုက်ရိုက်ဈေးကွက်လုပ်ငန်း (direct marketing) အတွက်ဆိုလျှင်၊ အပြည့်အဝ ဆန့်ကျင်ပိုင်ခွင့်ရှိသည်။

ဤတောင်းဆိုမှုများကို လက်ခံရရှိသည့်သူများသည် တုံ့ပြန်ရန် မလုပ်ဆောင်သင့်ဘဲ ကျောင်းအုပ်ထံ ဆက်သွယ်ရမည်ဖြစ်သည်။

အလိုအလျောက် ဆုံးဖြတ်ချက်ချခြင်းနှင့် ပရိုဖိုင်ပြုလုပ်ခြင်းဆိုင်ရာ အခွင့်အရေးများ

ဒေတာပိုင်ရှင်များအား အကျိုးသက်ရောက်မှုများ ကြီးစွာ ဖြစ်ပေါ်နိုင်သော အလိုအလျောက် ဆုံးဖြတ်ချက်ချခြင်းနှင့် ပရိုဖိုင်းလ်လုပ်ခြင်းများတွင်၊ ၎င်းတို့သည် ထိုဆုံးဖြတ်ချက်ကို

လူ့အဖွဲ့ဝင်တစ်ဦးမှ ပြန်လည်စစ်ဆေးရန် သို့မဟုတ် ထိုသို့သောဆုံးဖြတ်ချက်ချခြင်း မခံရစေရန် တောင်းဆိုခွင့်ရှိပါသည်။ဂင်းတို့၏ တောင်းဆိုချက်များကို ကျောင်းအုပ်ကြီးထံသို့ ချက်ချင်းပေးပို့ရမည်။

အချက်အလက်မျှဝေခြင်း။

ပုဂ္ဂိုလ်ရေးအချက်အလက်များကို ကျောင်းအတွင်း လွှဲပြောင်းသည့်အခါ၊ လက်ခံသူသည် အချက်အလက်စုဆောင်းခဲ့သည့် မူလရည်ရွယ်ချက်နှင့်အညီ အချက်အလက်ကိုသာ လုပ်ဆောင်ရပါမည်။ ကိုယ်ရေးကိုယ်တာအချက်အလက်ကို ရည်ရွယ်ချက်အသစ်နှင့် မတူညီသော ရည်ရွယ်ချက်တစ်ခုအတွက် ကျောင်းအတွင်းမျှဝေပါက၊ Data subject အား အချက်အလက်သတိပေးချက် (privacy notice) အသစ်ကို ထပ်မံပေးပို့ရမည် ဖြစ်သည်။

ပုဂ္ဂိုလ်ရေးအချက်အလက်များကို ပြင်ပသို့ လွှဲပြောင်းသည့်အခါ၊ ဥပဒေအရအခြေခံအချက်များကို ထည့်သွင်းစဉ်းစားရမည်ဖြစ်ပြီး၊ တတိယအဖွဲ့အကြား ဒေတာမျှဝေသဘောတူစာချုပ်ကို လက်မှတ်ရေးထိုး ရမည်ဖြစ်သည်။ သို့သော်၊ ဥပဒေအရ ဖော်ပြရန်လိုအပ်သောအခြေအနေများ - ဥပမာ၊ တရားဥပဒေအရ လိုအပ်သည့် အစိုးရဌာနများထံမှ တောင်းဆိုမှုရှိသည့်အခါတွင်၊ တတိယအဖွဲ့သည် ဥပဒေချမှတ်မှု ဆိုင်ရာရည်ရွယ်ချက်များအတွက် ဒေတာကို တောင်းခံနေပါက - ထိုသဘောတူစာချုပ်မလိုအပ်ပါ။

ပုဂ္ဂိုလ်ရေးအချက်အလက်များကို ပြည်ထောင်စုသမ္မတမြန်မာနိုင်ငံတော် ပြင်ပသို့ လွှဲပြောင်းမည် ဆိုပါက၊ ထိုဒေတာများ လုံခြုံစေရန် သင့်လျော်သောကာကွယ်မှုများ ရှိရမည် ဖြစ်သည်။ ပုဂ္ဂိုလ်ရေးအချက်အလက်များကို နိုင်ငံခြားသို့ လွှဲပြောင်းခြင်းတွင် ပါဝင်သူ ဝန်ထမ်းများသည်၊ ထိုလွှဲပြောင်းမှုကို သဘောတူမီအထိ သင့်လျော်သောလုံခြုံရေး အစီအမံများ ဆောင်ရွက်ထားရမည့်ဖြစ်ပြီး၊ သက်ဆိုင်ရာ မြန်မာနိုင်ငံ၏ ဥပဒေအညွှန်းများနှင့် လည်း ကိုက်ညီစေရမည်။

တိုက်ရိုက်ဈေးကွက်ရှာဖွေရေး

တိုက်ရိုက်ဈေးကွက်မြှင့်တင်မှု (Direct marketing) သည် တစ်ဦးချင်းပုဂ္ဂိုလ်များထံသို့ ထုတ်ကုန်များနှင့် ဝန်ဆောင်မှုများ ရောင်းချခြင်းနှင့်ပတ်သက်သည့် အကြောင်းအရာများသာမက၊ ရည်ရွယ်ချက်များနှင့် အကြံဉာဏ်စိတ်ကူးများကို မြှင့်တင်ခြင်းလည်း ပါဝင်သည်။ MISY အတွက်ဆိုပါက၊ ဤအရာများတွင် ပွဲအစီအစဉ်များအကြောင်း အသိပေးခြင်း၊ ရန်ပုံငွေရှာဖော်ဆောင်ခြင်း၊ ပစ္စည်းများ သို့မဟုတ် ဝန်ဆောင်မှုများ ရောင်းချခြင်း စသောအကြောင်းအရာများ ပါဝင်မည်ဖြစ်သည်။ ဈေးကွက်ရှာဖွေရေးသည် စာတိုက်၊ တယ်လီဖုန်းနှင့် အီလက်ထရွန်နစ် မက်ဆေ့ချ်များဖြင့် ဆက်သွယ်မှုကဲ့သို့သော ဆက်သွယ်ရေးပုံစံအားလုံးကို အကျုံးဝင်သည်၊ ယင်းမှာ အီလက်ထရွန်နစ်နည်းလမ်းများဖြစ်သည့် အီးမေးလ်များနှင့် စာတိုပေးပို့ခြင်းကဲ့သို့သော ဆက်သွယ်ရေးနည်းလမ်းအားလုံးကို အကျုံးဝင်သည်။ ကျောင်းသည် တိုက်ရိုက်ဈေးကွက်မြှင့်တင်ရေး လုပ်ငန်းဆောင်ရွက်မှုတစ်ခုချင်းစီလုပ်ဆောင်သည့်အခါတိုင်း၌၊ ကျောင်း၏ မူဝါဒနှင့် သက်ဆိုင်ရာအမျိုးသားဥပဒေများကိုလိုက်နာရမည်ဖြစ်သည်။ ထို့အပြင် တစ်ဦးခြင်းပုဂ္ဂိုလ်တစ်ဦးဦးမှ တိုက်ရိုက်ဈေးကွက်မြှင့်တင်မှုအား ရပ်ပေးရန် တောင်းဆိုလာပါက၊ တိုက်ရိုက်ဈေးကွက်မြှင့်တင်မှု လှုပ်ရှားမှုများ အားလုံးကို ရပ်ပေးရမည်။

ကျောင်းသည် ကျောင်းမူဝါဒနှင့်အညီ အမြဲတမ်းလိုက်နာကြောင်း သေချာစေရမည်ဖြစ်ပြီး၊ တိုက်ရိုက်ဈေးကွက်ရှာဖွေရေး လုပ်ဆောင်သည့်အခါတိုင်း၊ သက်ဆိုင်ရာ အမျိုးသားဥပဒေပြုချက်တစ်ရပ်ရပ်ကို ရပ်တန့်ရန် တစ်ဦးချင်းတောင်းဆိုပါက တိုက်ရိုက်ဈေးကွက်ရှာဖွေရေးလုပ်ငန်းအားလုံးကို ရပ်ဆိုင်းရမည်ဖြစ်သည်။

အချက်အလက်ကာကွယ်ရေး သင်တန်း
အချက်အလက် ကာကွယ်ရေးသင်တန်းအား နှစ်စဉ် ပို့ချသွားမည်ဖြစ်ပြီး ဝန်ထမ်းအားလုံး စတင်မိတ်ဆက်ခြင်းလုပ်ငန်းစဉ်၏ တစ်စိတ်တစ်ပိုင်းဖြစ်ပါမည်။

အချက်အလက်အကာအကွယ် ချိုးဖောက်မှု
MISYသည် ၎င်းကိုင်ဆောင်ထားသော ကိုယ်ရေးကိုယ်တာအချက်အလက်များအတွက် သင့်လျော်ပြီး အချိုးကျသော လုံခြုံရေးကို အာမခံရန် တာဝန်ရှိပါသည်။ ၎င်းတွင် ခွင့်ပြုချက်မရှိဘဲ သို့မဟုတ် ဥပဒေမဲ့ လုပ်ဆောင်ခြင်းမှ အချက်အလက်များကို အကာအကွယ်ပေးခြင်းနှင့် အချက်အလက်များ မတော်တဆ ဆုံးရှုံးခြင်း၊ ဖျက်ဆီးခံရခြင်း သို့မဟုတ် ပျက်စီးခြင်းမှ ကာကွယ်ပေးခြင်းတို့ ပါဝင်သည်။ ကျောင်းသည် အချက်အလက်ကာကွယ်မှုဆိုင်ရာ အဖြစ်အပျက်များကို ရှောင်ရှားရန် အစွမ်းကုန် ကြိုးစားနေသော်လည်း အချိန်အခါအလိုက် အမှားအယွင်းများ ဖြစ်ပေါ်လာနိုင်သည်။ ပုဂ္ဂိုလ်ရေးအချက်အလက်နှင့် ပတ်သက်သော ဖြစ်စဉ်များ ဖြစ်ပေါ်လာနိုင်သည့် ဥပမာများမှာ အောက်ပါအကြောင်းကြောင့် ဖြစ်နိုင်ပါသည် -

- အချက်အလက် သို့မဟုတ် စက်ပစ္စည်းများ ပျောက်ဆုံးခြင်း သို့မဟုတ် ခိုးယူခံရခြင်း။
- ခွင့်ပြုချက်မရှိသူများ အသုံးပြုနိုင်အောင် လုံခြုံရေးထိန်းချုပ်မှု မထိရောက်ခြင်း
- စက်ပစ္စည်းချို့ယွင်းခြင်း။
- ခွင့်ပြုချက်မရှိဘဲ ထုတ်ဖော်ခြင်း။
- လူ့အမှား။
- ကွန်ပျူတာစနစ်အားဖောက်ထွင်းတိုက်ခိုက်မှု။

ဒေတာကာကွယ်ရေးနှင့် ဆိုင်သောဖြစ်စဉ် တစ်ခုခု ဖြစ်ပေါ်လာပါက၊ ၎င်းကို ကျောင်း၏ ဒေတာ ကာကွယ်ရေးတာဝန်ခံထံသို့ အသိပေးရမည်ဖြစ်ပြီး၊ ၎င်းသည် ထိုဖြစ်စဉ်အား ဒေတာကာကွယ်ရေးချိုးဖောက်မှု ဟုတ်၊မဟုတ် ကို စုံစမ်းစစ်ဆေးပြီး ဆုံးဖြတ်မည် ဖြစ်သည်။ အစီရင်ခံရမည့် ဒေတာကာကွယ်ရေးချိုးဖောက်မှု တစ်ခု ဖြစ်ပေါ်လာပါက ၎င်းဖြစ်စဉ် ဖြစ်ပေါ်မှုကို သတိပြုသိရှိသည့်အချိန်မှ ၄၈ နာရီ အတွင်း ကျောင်းအုပ်ကြီး ထံသို့ ချက်ချင်းအသိပေးရမည် ဖြစ်သည်။

ဆက်စပ်မူဝါဒများ:
ကလေးသူငယ်အန္တရာယ်ကင်းရှင်းရေး မူဝါဒနှင့် လုပ်ထုံးလုပ်နည်းများ
ကျောင်းဝင်ခွင့်မူဝါဒ

ဆက်စပ်ဖောင်များ:

ပုဂ္ဂိုလ်ရေးအချက်အလက် လုံခြုံရေး အသိပေးစာ