**سياسة تصنيف البيانات بجامعة الباحة**

**النطاق:**

تنطبق أحكام هذه السياسة على جميع البيانات التي تتلقاها أو تنتجها أو تتعامل معها الجامعة مهما كان مصدرها، أو شكلها أو طبيعتها. وتتواءم هذه السياسة مع سياسات حوكمة البيانات الوطنية الصادرة من مكتب إدارة البيانات الوطنية وسياسات الهيئة الوطنية للأمن السيبراني ذات العلاقة، وبما لا يتعارض مع هذه السياسات ومع الأنظمة المرعية وما يصدر بشأنها من تعديلات.

**المبادئ الأساسية لتصنيف البيانات:**

**المبدأ الأول: الأصل في البيانات الإتاحة**

الأصل في البيانات أن تكون متاحة (في المجال التنمـوي) مـا لم تقتـضِ طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية، والسرية للغاية (في المجال السياسي والأمني) مالم تقتضِ طبيعتها أو حساسيتها مستويات أدنى من التصنيف والحماية.

**المبدأ الثاني: الضرورة والتناسب**

يتم تصنيف البيانات إلى مسـتويات وفقاً لطبيعتها، ومستوى حساسيتها، ودرجة أثرها مـع الأخذ بعين الاعتبار الموازنة بين قيمتها ودرجة سريتها.

**المبدأ الثالث: التصنيف في الوقت المناسب**

يتم تصنيف البيانات عند إنشائها أو حين تلقيها من جهات أخرى ويكون التصنيف خلال فترة زمنية محددة

**المبدأ الرابع: المستوى الأعلى من الحماية**

يتم اعتماد المستوى الأعلى من التصنيف عندما يتضمن محتوى مجموعة متكاملة من البيانات مستويات تصنيف مختلفة.

**المبدأ الخامس: فصل المهام**

يتم الفصل بين مهام ومسؤوليات العاملين - فيما يتعلق بتصنيف البيانات أو الوصول إليها أو الإفصاح عنها أو استخدامها أو التعديل عليها أو إتلافها - بطريقة تحول دون تداخل الاختصاص وتتلافى تشتيت المسؤولية.

**المبدأ السادس: الحاجة إلى المعرفة**

يتم تقييد الوصول إلى البيانات واستخدامها على أساس الاحتياج الفعلي للمعرفة، ولأقل عدد ممكن من العاملين.

**المبدأ السابع: الحد الأدنى من الامتيازات**

يتــم تقييــد إدارة صلاحيــات العامليــن علــى الحــد الأدنــى مــن الامتيــازات اللازمــة لأداء المهــام والمســؤوليات المناطــة بهــم.

**سياسة البيانات المفتوحة**

**النطاق:**

تنطبــق أحــكام هــذه السياســة علــى جميــع البيانــات والمعلومــات العامــة – غيــر المحميــة – التــي تنتجهــا جامعة الباحة مهمـا كان مصدرهـا، أو شـكلها أو طبيعتهـا – ويشـمل ذلـك السـجلات الورقيـة ورسـائل البريــد الالكترونــي والمعلومــات المخزنــة علــى الكمبيوتــر، أو أشــرطة الصــوت، أو الفيديــو، أو الخرائــط، أو الصــور الفوتوغرافيــة، أو المخطوطــات، أو الوثائــق المكتوبــة بخــط اليــد، أو أي شــكل آخــر مــن أشــكال المعلومــات المســجلة.

**المبادئ الأساسية للبيانات المفتوحة:**

**اﻟﻤﺒﺪأ اﻷول: اﻷﺻﻞ ﻓﻲ اﻟﺒﻴﺎﻧﺎت اﻹﺗﺎﺣﺔ**

يضمن هذا المبدأ إتاحة البيانات العامة الخاصة بالجامعة للجميع من خلال الإفصاح عنها، أو تمكين الوصول إليها، أو استخدامها، ما لم تقتض طبيعتها عدم الإفصاح عنها أو حماية خصوصيتها أو سرّيتها.

**اﻟﻤبدأ اﻟﺜﺎﻧﻲ: اﻟﺼﻴﻐﺔ اﻟﻤﻔﺘﻮﺣﺔ واﻣﻜﺎﻧﻴﺔ اﻟﻘﺮاءة آﻟﻴﺎ**

يتم إتاحة البيانات وتوفيرها بصيغة مقروءة آلياً ( (CSV , XLS , JSON , XML

**اﻟﻤﺒﺪأ اﻟﺜﺎﻟﺚ: ﺣﺪاﺛﺔ** **اﻟﺒﻴﺎﻧﺎت**

يتم نشر أحدث إصدار من مجموعة البيانات.

**اﻟﻤﺒﺪأ اﻟﺮاﺑﻊ: اﻟﺸﻤﻮﻟﻴّﺔ**

يجب أن تكون مجموعات البيانات المفتوحة شاملة وتتضمن أكبر قدر ممكن من التفاصيل وأن تعكس البيانات المسجلة بما لا يتعارض مع سياسة حماية البيانات الشخصية.

**اﻟﻤﺒﺪأ اﻟﺨﺎﻣﺲ: ﻋﺪم اﻟﺘﻤﻴﻴﺰ**

يجب إتاحة مجموعات البيانات للجميع دون تمييز ودون حاجة للتسجيل في المنصة.

**اﻟﻤﺒﺪأ اﻟﺴﺎدس: ﺑﺪون ﻣﻘﺎﺑﻞ ﻣﺎﻟﻲ**

يجب إتاحة البيانات المفتوحة للجميع مجاناً.

**اﻟﻤﺒﺪأ اﻟﺴﺎﺑﻊ: ﺗﺮﺧﻴﺺ اﻟﺒﻴﺎﻧﺎت اﻟﻤﻔﺘﻮﺣﺔ ﻓﻲ اﻟﻤﻤﻠﻜﺔ**

يجب أن تخضع البيانات المفتوحة لترخيص يحدد الأساس النظامي لاستخدام البيانات المفتوحة وكذلك الشروط والالتزامات.

**اﻟﻤﺒﺪأ اﻟﺜﺎﻣﻦ: ﺗﻄﻮﻳﺮ ﻧﻤﻮذج اﻟﺤﻮﻛﻤﺔ وإﺷﺮاك اﻟﺠﻤﻴﻊ**

تتيح البيانات المفتوحة عملية الاطلاع والمشاركة للجميع، وتعزز شفافية ومساءلة الجهات العامة، ودعم عملية صنع القرار وتقديم الخدمات.

**اﻟﻤﺒﺪأ اﻟﺘﺎﺳﻊ: اﻟﺘﻨﻤﻴﺔ اﻟﺸﺎﻣﻠﺔ واﻻﺑﺘﻜﺎر**

يجب تعزيز إعادة استخدام البيانات المفتوحة. كما يجب التكامل بين مختلف الجهات لإعداد جيل قادم من المبتكرين في مجال البيانات المفتوحة، وإشراك الأفراد والمؤسسات بوجه عام.

**سياسة حرية المعلومات**

**النطاق:**

ﺗﻨﻄﺒﻖ ﻫﺬه اﻟﺴﻴﺎﺳﺔ ﻋﻠﻰ ﺟﻤﻴﻊ ﻃﻠﺒﺎت اﻷﻓﺮاد ﻟﻼﻃﻼع أو اﻟﺤﺼﻮل ﻋﻠﻰ اﻟﻤﻌﻠﻮﻣﺎت اﻟﻌﺎﻣﺔ – ﻏﻴﺮ اﻟﻤﺤﻤﻴﺔ – اﻟﺘﻲ ﺗﻨﺘﺠﻬﺎ الجامعة ﻣﻬﻤﺎ ﻛﺎن ﻣﺼﺪرﻫﺎ، أو ﺷﻜﻠﻬﺎ أو ﻃﺒﻴﻌﺘﻬﺎ – وﻳﺸﻤﻞ ذﻟﻚ اﻟﺴﺠﻼت اﻟﻮرﻗﻴﺔ ورﺳﺎﺋﻞ اﻟﺒﺮﻳﺪ اﻹﻟﻜﺘﺮوﻧﻲ واﻟﻤﻌﻠﻮﻣﺎت اﻟﻤﺨﺰﻧﺔ ﻋﻠﻰ اﻟﻜﻤﺒﻴﻮﺗﺮ أو أﺷﺮﻃﺔ اﻟﺼﻮت أو اﻟﻔﻴﺪﻳﻮ أو اﻟﺨﺮاﺋﻂ أو اﻟﺼﻮر اﻟﻔﻮﺗﻮﻏﺮاﻓﻴﺔ أو اﻟﻤﺨﻄﻮﻃﺎت أو اﻟﻮﺛﺎﺋﻖ اﻟﻤﻜﺘﻮﺑﺔ ﺑﺨﻂ اﻟﻴﺪ، أو أي ﺷﻜﻞ آﺧﺮ ﻣﻦ أﺷﻜﺎل اﻟﻤﻌﻠﻮﻣﺎت اﻟﻤﺴﺠﻠﺔ.

ﻻ ﺗﻨﻄﺒﻖ أﺣﻜﺎم ﻫﺬه اﻟﺴﻴﺎﺳﺔ ﻋﻠﻰ اﻟﻤﻌﻠﻮﻣﺎت اﻟﻤﺤﻤﻴﺔ:

1. اﻟﻤﻌﻠﻮﻣﺎت اﻟﺘﻲ ﻳﺆدي إﻓﺸﺎؤﻫﺎ إﻟﻰ اﻹﺿﺮار ﺑﺎﻷﻣﻦ اﻟﻮﻃﻨﻲ ﻟﻠﺪوﻟﺔ أو ﺳﻴﺎﺳﺎﺗﻬﺎ أو ﻣﺼﺎﻟﺤﻬﺎ أو ﺣﻘﻮﻗﻬا.
2. اﻟﻤﻌﻠﻮﻣﺎت اﻟﻌﺴﻜﺮﻳﺔ واﻷﻣﻨﻴﺔ.
3. اﻟﻤﻌﻠﻮﻣﺎت واﻟﻮﺛﺎﺋﻖ اﻟﺘﻲ ﻳﺘﻢ اﻟﺤﺼﻮل ﻋﻠﻴﻬﺎ ﺑﻤﻘﺘﻀﻰ اﺗﻔﺎق ﻣﻊ دوﻟﺔ أﺧﺮى وﺗﺼﻨﻒ ﻋﻠﻰ أﻧﻬﺎ ﻣﺤﻤﻴﺔ.
4. اﻟﺘﺤﺮﻳﺎت واﻟﺘﺤﻘﻴﻘﺎت وأﻋﻤﺎل اﻟﻀﺒﻂ وﻋﻤﻠﻴﺎت اﻟﺘﻔﺘﻴﺶ واﻟﻤﺮاﻗﺒﺔ اﻟﻤﺘﻌﻠﻘﺔ ﺑﺠﺮﻳﻤﺔ أو ﻣﺨﺎﻟﻔﺔ أو ﺗﻬﺪﻳﺪ.
5. اﻟﻤﻌﻠﻮﻣﺎت اﻟﺘﻲ ﺗﺘﻀﻤﻦ ﺗﻮﺻﻴﺎت أو اﻗﺘﺮاﺣﺎت أو اﺳﺘﺸﺎرات ﻣﻦ أﺟﻞ إﺻﺪار ﺗﺸﺮﻳﻊ أو ﻗﺮار ﺣﻜﻮﻣﻲ ﻟﻢ ﻳﺼﺪر ﺑﻌﺪ.
6. اﻟﻤﻌﻠﻮﻣﺎت ذات اﻟﻄﺒﻴﻌﺔ اﻟﺘﺠﺎرﻳﺔ أو اﻟﺼﻨﺎﻋﻴﺔ أو اﻟﻤﺎﻟﻴﺔ أو اﻻﻗﺘﺼﺎدﻳﺔ اﻟﺘﻲ ﻳﺆدي اﻹﻓﺼﺎح ﻋﻨﻬﺎ إﻟﻰ ﺗﺤﻘﻴﻖ رﺑﺢ أو ﺗﻼﻓﻲ ﺧﺴﺎرة ﺑﻄﺮﻳﻘﺔ ﻏﻴﺮ ﻣﺸﺮوﻋﺔ.
7. اﻷﺑﺤﺎث اﻟﻌﻠﻤﻴﺔ أو اﻟﺘﻘﻨﻴﺔ، أو اﻟﺤﻘﻮق اﻟﻤﺸﺘﻤﻠﺔ ﻋﻠﻰ ﺣﻖ ﻣﻦ ﺣﻘﻮق اﻟﻤﻠﻜﻴﺔ اﻟﻔﻜﺮﻳﺔ اﻟﺘﻲ ﻳﺆدي اﻟﻜﺸﻒ ﻋﻨﻬﺎ إﻟﻰ اﻟﻤﺴﺎس ﺑﺤﻖ ﻣﻌﻨﻮي.
8. اﻟﻤﻌﻠﻮﻣﺎت اﻟﻤﺘﻌﻠﻘﺔ ﺑﺎﻟﻤﻨﺎﻓﺴﺎت واﻟﻌﻄﺎءات واﻟﻤﺰاﻳﺪات اﻟﺘﻲ ﻳﺆدي اﻹﻓﺼﺎح ﻋﻨﻬﺎ إﻟﻰ اﻹﺧﻼل ﺑﻌﺪاﻟﺔ اﻟﻤﻨﺎﻓﺴﺔ.
9. اﻟﻤﻌﻠﻮﻣﺎت اﻟﺘﻲ ﺗﻜﻮن ﺳﺮﻳﺔ أو ﺷﺨﺼﻴﺔ ﺑﻤﻮﺟﺐ ﻧﻈﺎم آﺧﺮ، أو ﺗﺘﻄﻠﺐ إﺟﺮاءات ﻧﻈﺎﻣﻴﺔ ﻣﻌﻴﻨﺔ ﻟﻠﻮﺻﻮل إﻟﻴﻬﺎ أو اﻟﺤﺼﻮل

ﻋﻠﻴﻬﺎ.

**المبادئ الأساسية لحرية المعلومات:**

**المبدأ الأول: المسؤولية**

أن يتــم تحديــد وتوثيــق سياســات وإجــراءات الخصوصيــة الخاصــة بالجامعة من قبل مكتب إدارة البيانات واعتمادهــا مــن رئيس الجامعة (أو مــن يفوضــه)، ونشــرها إلــى جميــع الأطــراف المعنيــة بتطبيقهــا.

**اﻟﻤﺒﺪأ الثاني: اﻟﺸﻔﺎﻓﻴﺔ**

للفــرد الحــق فــي معرفــة المعلومــات المتعلقــة بأنشــطة الجهــات العامــة تعزيــزاً لمنظومــة النزاهــة والشــفافية والمســاءلة.

**اﻟﻤﺒﺪأ اﻟﺜﺎلث: اﻟﻀﺮورة واﻟﺘﻨﺎﺳب**

أي قيـود علـى طلـب الاطلاع أو الحصـول علـى المعلومـات المحميـة التـي تتلقاهـا أو تنتجهـا أو تتعامـل معهـا الجهـات العامـة يجـب أن تكـون مسـوغة بطريقـة واضحـة وصريحـة.

**اﻟﻤﺒﺪأ اﻟرابع: اﻷﺻﻞ ﻓﻲ اﻟﻤﻌﻠﻮﻣﺎت اﻟﻌﺎﻣﺔ اﻹﻓﺼﺎح**

لـكل فـرد الحـق فـي الاطلاع علـى المعلومـات العامـة – غيـر المحميـة – وليـس بالضـرورة أن يتمتـع مقـدم الطلـب بحيثيـة معينـة أو باهتمـام معيـن بهـذه المعلومـات ليتمكـن مـن الحصـول عليهـا، كمـا ال يتعـرض ألي مسـاءلة قانونيـة متعلقـة بهـذا الحـق.

**اﻟﻤﺒﺪأ اﻟخامس: اﻟﻤﺴﺎواة**

يتــم التعامــل مــع جميــع طلبــات الاطلاع أو الحصــول علــى المعلومــات العامــة علــى أســاس المســاواة وعــدم التمييــز بيــن الأفــراد.

**سياسة حماية البيانات الشخصية**

**النطاق:**

 تنطبق أحكام هذه السياسة على جميع أنظمة جامعة الباحة ووحدات التحكم التي تقوم كلياً أو جزئياً بمعالجة البيانات الشخصية وكذلك الجهات الخارجية التي تقوم بمعالجة البيانات الشخصية المتعلقة بمنسوبي الجامعة والتي تتم عبر شبكة الإنترنت أو أي وسيلة أخرى. يستثنى من نطاق تطبيق هذه السياسة، جمع البيانات الشخصية من غير صاحبها مباشرة – دون علمه – أو معالجتها لغير الغـرض الذي جُمعت من أجله أو الإفصاح عنها دون موافقته أو نقلها إلى خارج المملكة في الأحوال التالية:

1. إذا كان جمــع البيانــات الشــخصية أو معالجتهــا مطلوبــاً لتحقيــق متطلبــات نظاميــة وفقــاً للأنظمــة واللوائــح والسياســات المعمــول بهــا فــي المملكــة أو لاســتيفاء مُتطلبــات قضائيــة أو لتنفيــذ التــزام بموجــب اتفــاق تكــون المملكــة طرفــاً فيــه.
2. إذا كان جمــع البيانــات الشــخصية أو معالجتهــا ضروريــاً لحمايــة الصحــة أو الســلامة العامــة أو حمايــة المصالح الحيوية للأفراد. ​

**المبادئ الأساسية لحماية البيانات الشخصية:**

**المبدأ الأول: المسؤولية**

أن يتــم تحديــد وتوثيــق سياســات وإجــراءات الخصوصيــة الخاصــة بالجامعة من قبل مكتب إدارة البيانات واعتمادهــا مــن رئيس الجامعة (أو مــن يفوضــه)، ونشــرها إلــى جميــع الأطــراف المعنيــة بتطبيقهــا.

**المبدأ الثاني: الشفافية**

أن يتم إعداد إشعار عن سياسات وإجراءات الخصوصية الخاصة بالجامعة يحدد فيه الأغراض التي من أجلها تمت معالجة البيانات الشخصية وذلك بصورة محددة وواضحة وصريحة.

**المبدأ الثالث: الاختيار والموافقة**

أن يتم تحديد جميع الخيارات الممكنة لصاحب البيانات الشخصية والحصول على موافقته (الضمنية أو الصريحة) فيما يتعلق بجمع بياناته واستخدامها أو الإفصاح عنها.

**المبدأ الرابع: الحد من جمع البيانات**

أن يقتصر جمع البيانات الشخصية على الحد الأدنـى مـن البيانات الـذي يمكّن من تحقيق الأغراض المحددة في إشعار الخصوصية.

**المبدأ الخامس: الحد من استخدام البيانات والاحتفاظ بها والتخلص منها**

أن يتم تقييد معالجة البيانات الشخصية بالأغراض المحددة في إشعار الخصوصية والتي من أجلها قدّم صاحب البيانات موافقته الضمنية أو الصريحة، والاحتفاظ بها طالما كان ذلك ضرورياً لتحقيق الأغراض المحددة أو لما تقتضيه الأنظمة واللوائح والسياسات المعمول بها في المملكـة وإتلافهـا بطريقة آمنة تمنع التسرب، أو الفقدان، أو الاختلاس، أو إساءة الاستخدام، أو الوصول غير المصرّح به نظاماً.

**المبدأ السادس: الوصول إلى البيانات**

أن يتم تحديد وتوفير الوسائل التي عن طريقها يمكن لصاحب البيانات الوصول إلى بياناته الشخصية لمراجعتها، وتحديثها، وتصحيحها.

**المبدأ السابع: الحد من الإفصاح عن البيانات**

أن يتــم تقييــد الإفصــاح عــن البيانــات الشــخصية للأطــراف الخارجيــة بالأغــراض المحــددة فــي إشــعار الخصوصيــة والتــي مــن أجلهــا قــدّم صاحــب البيانــات موافقتــه الضمنيــة أو الصريحــة.

**المبدأ الثامن: أمن البيانات**

أن تتم حماية البيانات الشخصية من التسرب، أو التلف، أو الفقدان، أو الاختلاس، أو إساءة الاستخدام، أو التعديــل، أو الوصــول غيــر المصــرّح بــه – وفقــاً لمــا يصــدر مــن الهيئــة الوطنيــة للأمــن الســيبراني والجهات ذات الاختصاص.

**المبدأ التاسع: جودة البيانات**

أن يتم الاحتفاظ بالبيانات الشخصية بصورة دقيقة، وكاملة، وذات علاقة مباشرة بالأغراض المحددة في إشعار الخصوصية.

**المبدأ العاشر: المراقبة والامتثال**

أن تتم مراقبة الامتثال لسياسات وإجراءات الخصوصية، ومعالجة الاستفسارات والشكاوى والنزاعات المتعلقة بالخصوصية. ​

**سياسة حماية بيانات الأطفال ومن في حكمهم**

**النطاق:**

تنطبق أحكام هذه السياسة على جميع أنظمة جامعة الباحة ووحدات التحكم التي تقوم كلياً أو جزئياً بمعالجة البيانات الشخصية للأطفال ومن في حكمهم بشكل كلي أو جزئي وبأي وسيلة سواء أكانت يدوية أو إلكترونية وكذلك الجهات الخارجية التي تقوم بمعالجة البيانات الشخصية للأطفال ومن في حكمهم المتعلقة بمنسوبي الجامعة والتي تتم عبر شبكة الإنترنت أو أي وسيلة أخرى.

# **القواعد العامة**

**دون إخلال بالقواعد العامة المنصوص عليها في سياسة حماية البيانات الشخصية، تلتزم جهة التحكم بالقواعد الإضافية التالية التي تضمن المحافظة على خصوصية الأطفال ومن في حكمهم وحماية حقوقهم:**

1. أن تكون جهة التحكم مسؤولة عن إعداد وتطبيق السياسات والإجراءات المتعلقة بحماية البيانات الشخصية للأطفال ومن في حكمهم، ويكون المسؤول الأول بالجهة -أو من يفوضه –مسؤولاً عن الموافقة عليها واعتمادها.
2. تلتزم جهة التحكم بتقييم الآثار السلبية والمخاطر المحتملة المترتبة على جميع أنشطة معالجة البيانات الشخصية للأطفال ومن في حكمهم، مع الأخذ بعين الاعتبار مصالحهم وحقوقهم وجميع ما يتعلق بأحوال أسرهم، وعرض نتائج التقييم على المسؤول الأول بالجهة -أو من يفوضه -لتحديد مستوى قبول المخاطر وإقرارها.
3. تلتزم جهة التحكم بمراجعة وتحديث العقود واتفاقيات مستوى الخدمة والتشغيل بما يتوافق مع السياسات والإجراءات المتعلقة بحماية البيانات الشخصية للأطفال ومن في حكمهم المعتمدة من الإدارة العليا للجهة.
4. تلتزم جهة التحكم بإعداد وتوثيق الإجراءات اللازمة لإدارة ومعالجة انتهاكات الخصوصية المتعلقة بالأطفال ومن في حكمهم وتحديد المهام والمسؤوليات المتعلقة بفريق العمل المختص والحالات التي يتم بها إشعار الجهة التنظيمية والمكتب حسب التسلسل الإداري بناء على قياس شدة الأثر.
5. تلتزم جهة التحكم بإعداد برامج توعوية لتعزيز ثقافة الخصوصية ورفع مستوى الوعي فيما يتعلق بجمع ومعالجة البيانات الشخصية للأطفال ومن في حكمهم.
6. تلتزم جهة التحكم بإعداد وتطوير إشعار الخصوصية بشكل واضح ودقيق وبلغة تناسب هذه الفئة ونشره على الموقع الإلكتروني أو التطبيق الخاص حسب الدليل الإرشادي لتطوير إشعار الخصوصية الصادر من المكتب) وإشعار الولي -بطريقة تناسب وقت جمع البيانات -بالغرض والأساس النظامي أو الاحتياج الفعلي والوسائل والطرق المستخدمة لجمع ومعالجة ومشاركة البيانات الشخصية للأطفال ومن في حكمهم وكذلك كيفية ممارسة الحقوق، والتدابير الأمنية لحماية خصوصيتهم، وأي تغييرات جوهرية تطرأ عليه.
7. تلتزم جهة التحكم بإشعار الولي عن المصادر الأخرى التي يتم استخدامها في حال تم جمع بيانات إضافية بطريقة غير مباشرة (من جهات أخرى).
8. تلتزم جهة التحكم بتزويد الولي بالخيارات المتاحة فيما يتعلق بمعالجة البيانات الشخصية للأطفال ومن في حكمهم والآلية المستخدمة لممارسة هذه الخيارات، ومنها على سبيل المثال. التفضيلات الشخصية التي من خلالها يمكن التعبير عن الرغبة في مدى مشاركة بياناتهم لأغراض أخرى.
9. تلتزم جهة التحكم بتبني مفهوم الخصوصية بالتصميم وبشكل افتراضي -يضمن مستوى الحماية دون تدخل مباشر من الطفل أو من في حكمه -عند تقديم الخدمات التي تستهدف هذه الفئة على وجه التحديد.
10. تلتزم جهة التحكم بأخذ موافقة الولي -التي يمكن التحقق منها بعد بذل الجهود المعقولة -على معالجة البيانات الشخصية للأطفال ومن في حكمهم بعد تحديد نوع الموافقة صريحة أو ضمنية بناءً على طبيعة البيانات وطرق جمعها.
11. أن يكون الغرض من جمع البيانات الشخصية للأطفال ومن في حكمهم متوافقاً مع الأنظمة ذات الصلة وذو علاقة مباشرة بنشاط جهة التحكم.
12. أن يكون محتوى البيانات مقتصراً على الحد الأدنى من البيانات اللازمة لتحقيق الغرض من جمعها.
13. أن يتم تقييد جمع البيانات الشخصية للأطفال ومن في حكمهم على المحتوى المعد سلفاً الموضح في القاعدة (12) ويكون بطريقة عادلة (مباشرة وواضحة وآمنة وخالية من أساليب الخداع أو التضليل).
14. أن يقتصر استخدام البيانات على الغرض الذي جمعت من أجله والذي تمت الموافقة عليه من قبل الولي.
15. تلتزم جهة التحكم بإعداد وتوثيق سياسة وإجراءات الاحتفاظ بالبيانات الشخصية للأطفال ومن في حكمهم وفقاً للأغراض المحددة والأنظمة والتشريعات ذات العلاقة.
16. تلتزم جهة التحكم بتخزين البيانات الشخصية للأطفال ومن في حكمهم ومعالجتها داخل الحدود الجغرافية للمملكة لضمان المحافظة على السيادة الوطنية على هذه البيانات، ولا يجوز معالجتها خارج المملكة إلا بعد حصول جهة التحكم على موافقة كتابية من الجهة التنظيمية أوفقاً للقواعد العامة لنقل البيانات الشخصية خارج الحدود الجغرافية للمملكة، بعد تنسيق الجهة التنظيمية مع المكتب متى ما استدعى الأمر ذلك.
17. تلتزم جهة التحكم بإعداد وتوثيق سياسة وإجراءات التخلص من البيانات لإتلاف البيانات بطريقة آمنة تمنع فقدانها أو إساءة استخدامها أو الوصول غير المصرح به -وتشمل البيانات التشغيلية المؤرشفة، والنسخ الاحتياطية -وذلك وفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني.
18. تلتزم جهة التحكم بتضمين أحكام سياستي الاحتفاظ والتخلص من البيانات في العقود في حال إسناد هذه المهام إلى جهات معالجة أخرى.
19. تلتزم جهة التحكم بتحديد وتوفير الوسائل التي من خلالها يمكن للولي الوصول إلى البيانات الشخصية للطفل ومن في حكمه وذلك لمراجعتها وتحديثها.
20. تلتزم جهة التحكم بالتحقق من هوية الولي قبل منحة الوصول إلى بيانات الطفل الشخصية ومن في حكمه وفقا للضوابط المعتمدة من قبل الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.
21. يحظر مشاركة البيانات الشخصية للأطفال ومن في حكمهم مع جهات أخرى إلا وفقا للأغراض المحددة بعد موافقة الولي ووفقاً للأنظمة واللوائح والسياسات ذات الصلة على أن يتم تزويد الجهات الأخرى بالسياسات والإجراءات المتعلقة بحماية البيانات الشخصية للأطفال ومن في حكمهم وتضمينها في العقود والاتفاقيات
22. تلتزم جهة التحكم بإشعار الولي وأخذ الموافقة منه في حال مشاركة البيانات مع جهات أخرى لاستخدامها في غير الأغراض المحددة.
23. تلتزم جهة التحكم بإشعار الولي في حال الرغبة في التواصل مع الطفل أو من في حكمه بطريقة مباشرة لأي غرض كان واتاحة الفرصة له لرفض هذا التواصل مع إيضاح كيفية قيامه بذلك.
24. تلتزم جهة التحكم بأخذ موافقة المكتب -بعد التنسيق مع الجهة التنظيمية – قبل مشاركة البيانات الشخصية للأطفال ومن في حكمهم مع جهات أخرى خارج المملكة.
25. يحظر على جهة التحكم جمع بيانات شخصية من الطفل أو من في حكمه تتعلق بأحد أفراد أسرته في أي حال من الأحوال، ماعدا البيانات الشخصية للولي.
26. تلتزم جهة التحكم بمتطلبات حماية خصوصية الأطفال ومن في حكمهم منذ المراحل الأولى من تصميم الخدمات والمنتجات التي تستهدف هذه الفئة، بما في ذلك المواقع الإلكترونية أو التطبيقات الرقمية.
27. تلتزم جهة التحكم بتطبيق التدابير المناسبة التي تمنع الأطفال ومن في حكمهم من إتاحة بياناتهم الشخصية والحساسة للجمهور بطريقة يمكن من خلالها التعرف عليهم وعلى أسرهم بشكل مباشر.
28. تلتزم جهة التحكم بتطبيق التدابير المناسبة والممكنة عملياً في حدود المعقول لحذف البيانات الشخصية والحساسة من منشورات الطفل ومن في حكمه قبل نشرها، بما في ذلك عرض الملفات الشخصية والنشر عبر حسابات التواصل الاجتماعي.
29. تلتزم جهة التحكم بعدم اتخاذ قرارات آلية بناء على معالجة البيانات الشخصية للأطفال ومن في حكمهم واستخدامها لأغراض متعددة لها تأثير كبير عليهم، ومنها على سبيل المثال التسويق المباشر.
30. تلتزم جهة التحكم باستخدام الضوابط الإدارية والتدابير التقنية والضمانات القانونية الكافية لحماية البيانات الشخصية للأطفال ومن في حكمهم.
31. تلتزم جهة التحكم بمراقبة الامتثال للسياسات والإجراءات المتعلقة بحماية البيانات الشخصية للأطفال ومن في حكمهم بشكل دوري ويتم عرضها على المسؤول الأول للجهة -أو من يفوضه -كما يتم تحديد وتوثيق الإجراءات التصحيحية التي سيتم اتخاذها في حال عدم الامتثال وإشعار الجهة التنظيمية والمكتب حسب التسلسل التنظيمي.

**سياسة مشاركة البيانات**

**النطاق:**

 تنطبق أحكام هذه السياسة على عمليات مشاركة البيانات التي تنتجها الجامعة - مع جهات حكومية أخرى أو جهات خاصة أو أفراد - مهما كان مصدر هذه البيانات أو شكلها أو طبيعتها.

لا تنطبق هذه السياسة في حال كانت الجهة الطالبة للبيانات جهة حكومية وكان الطلب لأغراض أمنية أو لاستيفاء متطلبات قضائية.
 تتواءم هذه السياسة مع سياسات حوكمة البيانات الوطنية الصادرة من مكتب إدارة البيانات الوطنية وبما لا يتعارض معها ومع الأنظمة المرعية وما يصدر بشأنها من تعديلات.

**المبادئ الأساسية لمشاركة البيانات:**

**اﻟﻤﺒﺪأ اﻷول: ﺗﻌﺰﻳﺰ ﺛﻘﺎﻓﺔ اﻟﻤﺸﺎرﻛﺔ**

 تقوم المؤسسة بمشاركة البيانات الرئيسية التي تنتجها وذلك لتحقيق التكامل بينها وبين الجهات الأخرى وتبني مبدأ "المرة الواحدة" للحصول على البيانات من مصادرها الصحيحة والحد من ازدواجيتها وتعارضها وتعدد مصادرها. وفي حال تم طلب البيانات من غير مصدرها الأساسي، فيتم أخذ موافقة الجهة الرئيسية \_مصدر البيانات\_ قبل مشاركتها مع الجهة الطالبة.

**اﻟﻤﺒﺪأ اﻟﺜﺎﻧﻲ: ﻣﺸﺮوﻋﻴﺔ اﻟﻐﺮض**

 أن يتم مشاركة البيانات لأغراض مشروعة مبنية على أساس نظامي أو احتياج عملي مسوغ يهدف إلى تحقيق مصلحة عامة دون إلحاق أي ضرر بالمصالح الوطنية، أو أنشطة الجهات، أو خصوصية الأفراد، أو سلامة البيئة – ويستثنى من ذلك البيانات والجهات المستثناة بأوامر سامية.

**اﻟﻤﺒﺪأ اﻟﺜﺎﻟﺚ: اﻟﻮﺻﻮل اﻟﻤﺼﺮح ﺑﻪ**

 أن يكون لدى جميع الأطراف المُشارِكة في مشاركة البيانات صلاحية الاطلاع على هذه البيانات والحصول عليها واستخدامها (والتي قد تتطلب المسح الأمني حسب طبيعة وحساسية البيانات)، بالإضافة إلى المعرفة، والمهارة، والأشخاص المؤهلين والمدربين بشكل صحيح للتعامل مع البيانات المشتركة.

**اﻟﻤﺒﺪأ اﻟﺮاﺑﻊ: اﻟﺸﻔﺎﻓﻴﺔ**

 يجب على جميع الأطراف المُشارِكة في عمليات مشاركة البيانات إتاحة جميع المعلومات الضرورية لتبادل البيانات بما في ذلك: البيانات المطلوبة، الغرض من جمعها، ووسائل نقلها، وطرق حفظها، والضوابط المستخدمة لحمايتها وآلية التخلص منها.

**اﻟﻤﺒﺪأ اﻟﺨﺎﻣﺲ: اﻟﻤﺴﺆوﻟﻴﺔ اﻟﻤﺸﺘﺮﻛﺔ**

 أن تكون جميع الأطراف المُشارِكة في مشاركة البيانات مسؤولة مسؤولية مشتركة عن قرارات مشاركة البيانات ومعالجتها وفقاً للأغراض المحددة وضمان تطبيق الضوابط الأمنية المنصوص عليها في اتفاقية مشاركة البيانات، والأنظمة والتشريعات والسياسات ذات العلاقة.

**اﻟﻤﺒﺪأ اﻟﺴﺎدس: أﻣﻦ اﻟﺒﻴﺎﻧﺎت**

 أن تقوم جميع الأطراف المُشارِكة في مشاركة البيانات بتطبيق الضوابط الأمنية المناسبة لحماية البيانات ومشاركتها في بيئة آمنة وموثوقة وفقاً للأنظمة والتشريعات ذات العلاقة، ووفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني.

**اﻟﻤﺒﺪأ اﻟﺴﺎﺑﻊ: اﻻﺳﺘﺨﺪام اﻷﺧﻼﻗﻲ**

 أن تقوم جميع الأطراف المُشارِكة في مشاركة البيانات بتطبيق الممارسات الأخلاقية أثناء عملية مشاركة البيانات لضمان استخدامها في إطار من العدالة والنزاهة والأمانة والاحترام، وعدم الاكتفاء بالالتزام بسياسات أمن المعلومات أو الالتزام بالمتطلبات التنظيمية والتشريعية ذات العلاقة.