情報セキュリティ対策基準

～ 情報セキュリティ・ポリシー ～

公益財団法人豊中市スポーツ振興事業団

はじめに

この基準は、当財団で管理運営する各館にて執り行う各種スポーツ教室及び施設の利用に係るお客様の個人情報取り扱い、ならびに当事業団で従事する職員の個人情報取り扱い、さらに、それらの事務処理に使用する各種情報機器端末の管理及び取扱いについて、当事業団の「個人情報保護に関する要綱」に基づき、詳細な行動基準を定めたものである。

《目　　次》

（1）情報保護管理者

情報の保護及び管理に関して、当事業団に次の担当者を置き、その権限と責任を明確にし、情報セキュリティ・ポリシーの周知・徹底を図る。

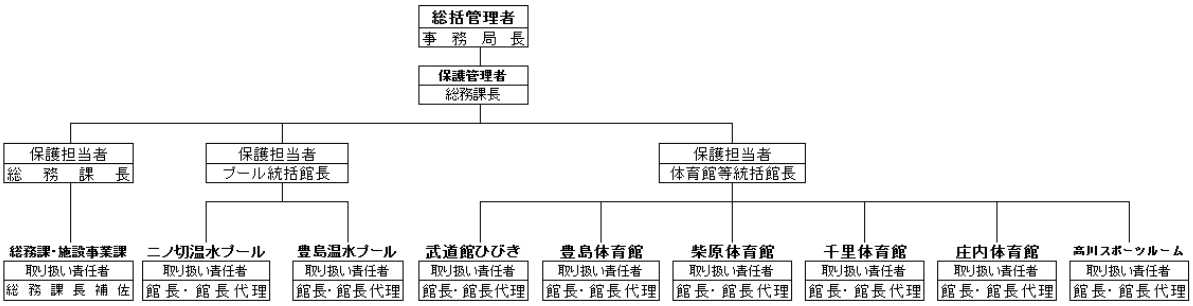
【総括管理者】　事務局長
- ・情報セキュリティの管理責任者として、保有情報を適切に管理する。
- ・情報保護、適正管理、及びセキュリティ対策実施に関する基本的事項を統括する。
- ・情報セキュリティ会議の招集を行う。

【保護管理者】　総務課長
- ・情報保護、適正管理、及びセキュリティ対策の実施について統括、管理する。
- ・情報セキュリティ会議の議長を務める。
- ・豊中市、所轄課、及び関係団体との連絡調整を行う。

【保護担当者】　プール統括館長、及び体育館等統括館長
- ・所管する課の情報を適正に管理し、及びその取扱いについて必要な措置を講じる。
- ・同情報のセキュリティに関するＩＤ及びパスワードを適正に管理する。
- ・電磁的記録媒体等の引渡し、受領その他必要な事項を記録する。
- ・保有する分類されたデータが記録されている電磁的記録媒体等を適正に管理し、又は廃棄する。
- ・所有するシステム、アプリケーションソフト、その他これらに類するもの（以下「ドキュメント」という。）を、厳重かつ適切に保管する等適正に管理する。
- ・ドキュメントの複写又は外部への持ち出しを承認、及び記録を行う。
- ・パソコン機器等の運用に関し影響が生じるときは必要な調整を行う。
- ・パソコン機器等の故障その他の事故、火災その他の事故、不正行為、不正アクセス行為又はデータの漏えい若しくは紛失（以下これらを「事故等」という。）を発見した場合は、速やかに保護管理者へ報告する。
- ・保有する分類されたデータが記録されている電磁的記録媒体等を適正に管理し、又は廃棄する。
- ・個人情報に係る電算処理を依頼しようとするときは、その収集方法及び目的外利用又は外部提供に関する事項を保護管理者に通知する
- ・パソコン機器等の導入、運用及び保守その他電算処理の事務を委託しようとするときは、データの保護その他セキュリティ対策について必要な事項を明記して契約する。

【取り扱い責任者】館長、課長代理、及び館長代理
- ・所管する施設において、パソコン機器等を適正に管理し、及びその操作その他の取扱いについて必要な措置を講じる。
- ・ID 及びパスワードの管理について必要な措置を講じる。
- ・保有する分類されたデータが記録されている電磁的記録媒体等を適正に管理し、又は廃棄する。

≪情報セキュリティ管理体制図≫



※ 別表１　「公益財団法人豊中市スポーツ振興事業団　情報管理体制図」参照

（2）情報収集時の守るべき事項

個人情報を収集する際には、次のことを守ることとする。

【利用目的の明確化、通知、公表】
利用目的を明記し、当該者に通知すること。また、問い合わせ先を記しておくこと。

例)「アンケート」等で、情報を収集する場合

・このアンケート（調査）は、○○○○のために利用します。回答者の住所・氏名などの個人情報は、本校からの案内等の発送（緊急連絡）のために使用し、目的外に利用することはありません。
・アンケートで収集した個人情報は（厳重に管理します。また、本人の同意を得ることなく、）第三者に開示・提供することはありません。
〈本アンケート（調査）に対する問い合わせ先〉
公益財団法人豊中市スポーツ振興事業団

【利用目的に関係しない情報は収集しない】
「緊急連絡網」→TEL.のみで対応でき、郵便物等を利用しないのなら、現住所、〒番号等は必要ない。「念」のためとか、「とりあえず」といった発想を捨てて、絞り込むこと。

（３）入室制限、施錠、保管場所等

個人情報は、重要な「資産」であり、情報保管場所への勝手な出入りを許すことは、個人情報保護にとって非常に危険なこととなる。

【入退出】
入札作業や採用期間中など、施設内（事務所）への入退出に際しては、以下のルールを設けることとする。

・荷物の受け渡しに際しては、事務所前を原則とするが、状況によっては、職員立ち会いのもと必要な場所に搬入してもらう。

【鍵管理】

個人情報保護に限らず、鍵の管理は極めて重要であることを認識すること。

・機械警備のカードの取扱は十分注意する。

・委託業者と施設の鍵を共有する場合、事前に両者立ち会いのもと、「鍵受渡し表」を作成し、引き渡し時、引き継ぎ時に確認する。

・割り当てられた自身の鍵を、施設職員であっても交換及び貸し借りを行わない。

・事務所内にある保管庫については施錠し、鍵の保管場所を共有する。

・金庫の使用については、複数個所に鍵を分散する。

・金庫及び手提げ金庫のセットキーを共有する。

・自身の業務机において、個人情報を取り扱う書類がある場合は、必ず施錠する。

・割り当てられたパソコン機器など、自身の施錠できる業務机で管理する。

【入出禁止について】

個人情報にふれる機会が多いため、次の部屋への・関係業者・利用者・保護者の入出を禁止する。入出禁止でない部屋の場合も入出にあたっては必ず関係者の許可が必要となる。

・事前連絡のない関係者以外の事務所内立ち入り禁止

・定められた期間（採用試験・入札・人事等）における事務所内立入禁止

【保管と整理整頓について】

個人情報保護のためには、各種データの整理整頓に努めることとする。

・重要な個人情報は、保管庫か、施錠できる引出に入れる。
・重要な文書を起案書類等で回覧する場合、必ず専用のファイルを使用する。
・机上を整頓し、個人情報が他書類に紛れ込まないようにする。
・ファックス、プリンター、コピー機は、できるだけ取扱い責任者の目の届くところに設置する。
・ファックス、プリンター、コピー機等に個人情報に関する用紙を出力したときは、放置せず、速やかに回収する。
・帰宅時は、施錠及びコンピュータ、ファックス、プリンター、コピー機周辺を点検する。

（4）ネットワーク利用等の遵守事項

コンピューターネットワークの利用は業務に便利な反面、「うっかりミス」や「ずさんな使用」が、莫大な個人情報の漏洩を招く危険性があるため、取り扱いには十分注意すること。

【パスワードとログオフ】

■パソコン機器など、起動時からパスワードを設定する。
■無線 LAN(WiFi)のパスワード設定は、定期的に変更する。
■共有フォルダを設定する際は、アカウント・パスワードを定期的に変更する。

・パスワードは少なくとも６文字以上、大小英文字と数字を組合せるのが望ましい。名前、生年月日、電話番号、車のナンバー等、推測されやすい文字を含むことを避ける。
・パスワードは定期的に変更する。また、絶対他人に漏らさないこと。メモもさける。
・部屋をでるときは必ずログオフをする。
・たとえ緊急事態であっても、職員のパソコンを利用者に使用させない。
・職員間のパソコン機器の交換、貸し借りは行わない。

【写真掲載時の注意】

ホームページ・SNS 等に写真を掲載する時は、下記の点に注意する。

・特定個人が判別できないように、顔などが鮮明に映らないように配慮する。また個人名を付記しない。
・個人の判定できる写真を掲載する場合は、必ず本人の許可を得る。
・概要などに、撮影の事前告知を行う。

【メール、インターネット利用時】

メール、インターネット利用時にも度々問題が生じる。メールは「公文書」であることを認識し、次のことを厳守すること。

・インターネットやメールの私的利用は原則禁止。
・私的なアカウントを設定しない。
・メールアドレス帳に、業務以外のメールアドレスは掲載しない。
・パソコン上に、アカウントやパスワードなど重要な情報を保存する設定にしない。
・メール送信の際は、送信先を再確認する。
・施設宛や職員宛に送付された公的メールを、許可なく他人のメールアドレスに送付することは禁止。
・送付対象者が限定されており、メーリングリストがある場合は、メーリングリストを利用すること。個々人のアドレスをピックアップして、送付しない。
・送信先メールアドレスのチェックを厳格にする。とくに、BCC で送付すべき所を、TO や CC で送らない。
・自動開封設定を解除しておく。
・プレビュー表示を行わない。
・見知らぬアドレスからのメールを安易に開封しない。
・見知らぬアドレスからの添付ファイルを開かない。
・送信者として送付する際、必ず件名に用件と宛名を記入する。
・プラグイン（便利ツール等のソフト）を安易に行わない。
・社内情報を個人の所有するソーシャルネットワークサービス等に、許可なく掲載することを禁止する。

【アプリケーションソフト等の取扱いについて】
支給されたパソコン機器の利用時は、次のことを厳守してください。

・インターネット上等で無料配布されているフリーアプリケーションソフトは使用してはならない。
・支給時にインストールされているアプリケーションソフト以外に、許可なく他のアプリケーションソフトをインストールしてはならない。
・業務上必要なアプリケーションソフトの導入を行うときは、事前に上司の許可、若しくは、起案による決裁を受けたものに限る。
・認証要件が定められたアプリケーションソフトを、不正に複数台のパソコンにインストールしてはならない。
・インターネット上等で、認証作業やアプリケーションソフト情報を登録する場合は、事前に上司の許可、若しくは、起案による決裁を受けるとともに、備品管理台帳へ記載すること。

【社内情報共有ソフト（office365）の使用について】
アプリケーションソフトの使用にあたっては、次のことを厳守してください。

・誤った操作や記載等による情報錯誤を防ぐため、別添の「office365 マニュアル」に基づき、適正に操作を行うこと。
・操作にあたって、問題が生じた場合や不備が発見された場合は、速やかに施設長（取扱い責任者）に報告するとともに、不用意な操作は行わないこと。
・付与されたメールアドレスの使用については、当対策基準「(18)メールのルール」に定められたとおり適正に使用すること。

（５）取扱者の限定、複製等の制限

書面やデジタルデータなど、保有個人情報については、取扱者を限定し、複製等を制限して、情報が不必要に拡散することを避けること。

【取扱者の限定】

・黒いデスクトップパソコンで共用して使用する場合（管理パート職員）は、「権限者 ID・パスワード」を設定し、定められた ID・パスワードにおいて使用する。
・「保有個人情報」ごとに、別途「取扱い責任者」「取扱者」を定めるが、「取扱者」に認定されていない場合は、情報を取り扱うことができない。
・「保有個人情報」が書面の場合、紛失、消失に特に気をつける必要がある。
・連絡網、各種名簿等、以外に「取扱者」が出る場合は、可能な限り対象者を絞るとともに、利用時の注意事項等を明記したうえで配布する。

【複製等の制限】

・複製を作成するときは、可能な限り対象者をしぼるとともに、重要な情報の場合は、通し番号を打った上で、誰に配布したかを記録する。

【連絡網等配布時の注意】

各種名簿・連絡網等については、事務所内の見える場所に掲示するのではなく、配布者を把握したうえで配布するか、共有できる場所に保管する。

例)「○○連絡網」につきましては、少なくとも今年度は、従来通り作成することになりました。なお、法律との関係から、以下の点ご留意下さい。
(1) この連絡網は、あくまで「○○体育館内の緊急連絡」のためにご利用下さい。
(2) 目的外に使用したり、連絡網に記載されている電話等の個人情報を第三者に漏らすことは、法律で禁止されています。
(3) この連絡網は、年度末には回収する予定ですので、厳重に保管されるようお願いします。

（６）個人機器持込、情報(機器)搬出の原則

【個人機器持込】

私用パソコン、モバイル機器、記録媒体等の持込は禁止する。

【施設の機器の持出】

施設のノートパソコン等の施設外への持出しは禁止とする。

【情報（機器）搬出の原則】

ここでいう「搬出」とは、パソコン機器本体、紙媒体の他、フロッピー等による搬出も含む。

１．提出書類は持出してよいが、事前に上司の許可、若しくは、起案による決裁を受けたものに限る。

２．持ち出せないもの。
→「教室参加者に関する書類」～申込書、受講者一覧表、名簿、健康調書等
「採用関係書類」～履歴書、申込書、採用結果、評価表等
「入札に関する書類」～業者一覧表、入札書等
「人事に関する書類」～職員名簿、住所録、給与等一覧表、勤務成績表、マイナンバー
上記内容に類するもの

３．持ち出しが必要となった場合の手順
→別紙申請書『施設外への情報（機器）搬出について（申請)』に、持ち出しの必要な情報内容、情報機器、その他必要事項を記入し、施設長に提出する。施設長は、総務課長に持ち出しを行う期日までに申請書を提出する。

（７）保有個人情報の第三者への提供

原則として、「個人情報保護に関する要綱」に従うこととする。

（８）業務委託時の取り決め

原則として「個人情報保護に関する要綱」に従うとともに、適正な業務委託先を選ぶため、契約書面で以下の個人情報に関する事項について確認を交わす。また、契約期間中は必ず契約書を保管しておくこと。

① 委託者及び受託者の責任の明確化、管理状況の検査に関する事項
② 委任契約範囲外の加工・利用、複写、複製の禁止
③ 個人データの漏洩防止、盗用防止及び事案の発生時の対応に関する事項
④ 委託契約期間及び契約終了後のデータの返還・消去・廃棄に関する事項
⑤ 再委託の制限または条件に関する事項
⑥ 違反した場合における契約解除の措置に関する事項

（９）個人情報取扱記録、保管期間、廃棄手順

【個人情報取扱い記録】

起案文書においては、保存年限に応じて、書類の保管・整理を行う。

【廃棄時のルール等】

「ゴミ」になると価値のないものと判断せず、廃棄時には、個人情報を復元不可能な状態にして、廃棄すること。

① 個人情報が含まれる「紙媒体」の場合、シュレッダーにかけることを基本とする。

② 古紙利用に際し注意が必要。個人情報の記された用紙を、不用意に再利用に回さない。

③ 個人情報を含む大量の書類を廃棄する場合は、豊中市による「溶解文書」収集にあわせて廃棄する。

④ デジタル媒体の廃棄にあたっては、メディアシュレッダーを利用するか、業者に廃棄を依頼する。

⑤ 古くなったパソコン機器の廃棄については、独断で廃棄せず、複数確認のもと業者による廃棄を依頼する。

（10）情報開示への対応

保有個人情報の開示等の措置については、当事業団の「情報公開要綱」に従い、実施する。保有個人情報の訂正及び利用停止、異議申し立てに関することも、同様とする。

（11）緊急時対応、事案の報告

個人情報漏洩等の問題が発生した場合は、次のような緊急対応をとる。まず、事案の発生を知った職員はいち早く対象者に連絡すること。次いで事務局長及び各施設長が事案をいち早く把握し、職員が正しい認識を共有すること。

【事案の連絡ルート】（勤務時間外、休日を含む）

発見者　→　施設長　→　総務課長　→　事務局長

※必要に応じて、所管課（スポーツ振興課）、弁護士、監督官庁、業務委託先等と連絡をとる

（12）遵守義務と罰則

《遵守義務》
職員は、下記に上げる事項について、情報セキュリティ対策を遵守すること。

① **「情報」収集時の注意**
- 利用目的を明記し、当該者に通知する。また、問い合わせ先を記しておく。
- 利用目的に関係しない情報は収集しない。

② **「名簿」等の管理**
- 施設から持出す際は、理由を明確にし、施設長の許可を得ること。
- 各種連絡網は電話等の必要最小限の情報掲載にとどめ、目的外使用禁止や廃棄手順について、連絡網に掲載する。

③ **「保管場所」等**
- 各種個人情報保護に関して定めている「取扱者の限定」「入出禁止」「施錠」等の措置を厳守のこと。

④ **「パソコン」使用時の留意点**
- パスワードの設定は慎重に。
- 部屋を出るときは、必ずログオフをすること。
- メール発信時には、注意事項および「電子メール運用マニュアル」を遵守すること。

⑤ **「ノートパソコン・モバイル機器」等の持込に関して**
- 個人の情報機器の職場への持ち込みは禁止する。

⑥ **「搬出」に関して**
- USB メモリ、フロッピー等に個人情報をコピーし持出禁止。
- 提出書類等、紙類の持ち出しは、施設長の許可、若しくは起案決裁をとり行う。
- インターネット上のファイル共有（ドロップボックス等）は行わない。

⑨ **データ廃棄時の注意**
- マニュアルにしたがって、情報毎に定められた方法（シュレッダー、業者委託等）で確実に廃棄する。

⑩ **事案発生時の対応**
- 休日であっても、いち早く施設長若しくは総務課長に連絡する。
- 招集がかかれば、直ちに出勤し、状況認識を共有する。
- 被害の拡大を防止するため、インターネットからの接続を切断する。

《罰則》

上記の遵守事項、及び、本対策基準に掲げる各事項に違反した者は、原則として罰則を科す。基本罰則は教育的指導及び権限の移動とするが、個人の責任によって、情報セキュリティに重要な影響を与える行為、個人のプライバシー侵害に該当する行為、資産喪失を招く悪質な行為を犯した場合は、理事会で協議の上、職務規定上の処分を科す。

手　順

①遵守義務が疑われる事象が発生した場合、保護管理者は、保護担当者または保護責任者に、調査の指示を行う。

②保護担当者または保護責任者は、調査指示を受け、事実確認を行い、速やかに保護管理者に報告する。

③保護管理者は、調査報告を受けて、必要な是正処置を指示する。ただし、是正処置を引き続き怠った場合や遵守義務違反が組織における情報セキュリティ上重大な事象の場合は、懲戒等審査会を開催し、必要な処分を行う。

（13）コンピュータ端末の管理

職員の利用しているコンピュータ端末が適切に管理されないことで、個人情報などのデータが流出が考えられる。「備品管理台帳」を基本とし、内容を随時更新しながら管理するとともに、職員が十分に注意して、コンピュータを自己管理すること。

【端末利用者による管理】

■「備品管理台帳」により定められたパソコン機器等の使用者は、定められた機器以外の使用は原則として禁止する。（貸し借りの禁止）
■コンピュータ端末からのログイン時には、パスワードを必要とする設定にする。
■コンピュータ端末のハードディスクに、個人情報のデータを保存するのは、原則として禁止する。やむを得ず個人情報をコピーしなければならない場合は、施設長の許可を得る。
■離席、帰宅の際には、必ずログオフすること。
■帰宅の際には、コンピュータ端末の電源を落とし、ノートパソコンは施錠できる場所に保管すること。
■コンピュータ端末の施設外への持ち出しは禁止する。やむを得ない場合は、盗難等の事態を想定し、不必要な情報は消去した上で、施設長の許可を得て、持ち出す。
■たとえ緊急事態であっても、職員用パソコンを利用者に使用させない。
■コンピュータ端末へのアプリケーションソフトのインストールを行いたい場合は、施設長の許可を得て実施すること。
■オペレーションシステムは、「自動更新」設定とし、施設長から特段の指示がない限り、設定を変更せず、常時最新のパターンファイルをインストールできる状態にしておく。
■アプリケーションソフト等のアップデート（更新）通知が来た場合は、施設長の許可を得て実施するものとする。不明瞭な場合は、自己判断せず、施設長に報告する。

（14）データの管理

コンピュータ上で、管理するデータは細心の注意を払い、運用すること。

【データベースの管理】

■施設長は、データへのアクセス制限をかける。
■施設長は、各種データのバックアップの頻度・手順を定めて、定期的に実行する。
■バックアップを保存した記録媒体は、厳重に管理する。
■施設長は、システムやデータが損壊したときの復旧手順を明確にしておく。

【データ運搬・記録媒体の管理】

■メール添付での個人情報の送信は、原則として禁止する。やむを得ずメール添付する場合は、暗号化やパスワードによる保護をかける。
■個人情報を記録媒体（CD-R･DVD-R･HDD･フラッシュメモリー等）にコピーして施設外に搬出することは、原則として禁止する。やむを得ない場合施設長に許可を得て、使用目的を達成した後には、速やかにデータを消去すること。
■個人情報を記録媒体（CD-R･DVD-R･HDD･フラッシュメモリー等）にコピーし持ち出す時は、施設長の許可を得ること。その場合、使用目的を達成した場合には、速やかにデータを消去すること。

【データの廃棄】

■パソコンを廃棄するときは、ハードディスクを物理的に破壊するか、専用のソフトウェアでデータを上書きして完全に消去する。
■記録媒体を廃棄するときは、メディアシュレッダー等で物理的に破壊する。

（15）パスワードの管理

情報化社会では、パスワードは非常に重要なため、パスワードに関する理解を深め、管理を徹底できるようにすること。

【パスワードの管理】

■パスワードは少なくとも 6 文字以上、英文字と数字を組合せるのが望ましい。氏名、生年月日、電話番号、車のナンバー等、推測されやすい文字を含むことを避ける。
■パスワードは、少なくとも 3 か月に一度、定期的に変更する。また絶対、他人に漏らさないこと。メモもさける。
■パスワード入力時に、手元を見られないように注意する。

【覚えやすく安全なパスワードの作成方法】

■パスワードは、英数字だけではなく記号などを取り入れると解読されにくくなる。次の例を参考に、各自で作成しましょう。

（例１）覚えやすい英数字を、英数字・記号に置き換える
　1983 年 5 月 19 日生まれ
　8305119→83May19→83mten91→53-m-ten9
（例 2）気に入っている文章などから、それぞれの語の頭文字をとる。
　私のペットの名前はトラとモモです。
　Watashi No Pet No Namae Ha Tora To Momo Desu
　→wnpnnhttmd→wnpn2ht2md→wnpn2-ht2-md

（16）コンピュータウィルス対策

コンピュータが１台でもコンピュータウィルスに感染すると、個人情報が流出するなど、被害は組織内だけで収まらずに大変な事態となる可能性が大きい。十分すぎるほどの対策を講じることが必要となる。

【感染予防】

■ウィルス対策ソフトをすべてのコンピュータ端末に導入する。
■ウィルス対策ソフトが、自動的に毎日パターンファイルを更新する設定にしておく。
■心当たりのない添付ファイルのあるメールは、開封せずに直ちに消去する習慣をつけ、確実に消去する。
■システムのアップグレードやプログラムの更新は「自動更新」とし、施設長から特段の指示がない限り、設定を変更してはならない。
■インストール済みのソフトから更新の通知が来た場合は、施設長の指示により更新作業を行う。

【危機管理】

■コンピュータウィルスの感染に気づいた場合は、直ちにコンピュータから LAN ケーブルを抜き、施設長に連絡する。
■施設長は、総務課長へ連絡し、情報セキュリティ対策本部を設置し、以下の手順で危機管理にあたる。

1. 直ちに外部へのネットワークを遮断する。
2. システム管理者を中心に、感染状況の把握、感染原因の究明、ウィルスの駆除を行う。
3. 必要ならば豊中市・所管課へ応援を要請する。

（17）個人機器・媒体持込のルール

■業務における備品購入時は、備品管理台帳に記載し、適切な管理を行う。

■備品管理台帳は、常に最新の状態とし、機器の設置、交換、損壊、紛失等により変更した場合は、速やかに更新作業を総務課において行う。

■私用ノートパソコン、モバイル機器、記録媒体等の持込は禁止する。「備品管理台帳」に掲載された機器以外の使用は行わない。　　ただし、私用スマートフォンについては、持ち込みは可能とするが、メール・予定表などの同期等を行うなど、データの持ち込み・持ち出し行為は禁止する。

（18）メールのルール

メール・インターネットは、日常業務に一般化され、便利なものとなっているが、反面セキュリティ意識の低下も起きやすい。情報の受発信の窓口にあたることから、その運用は十分に注意すること。

【メールのルール】

■メールアドレスの付与は、保護管理者で作成する。
■別表１に定められたメールアドレスを主として使用する。
- zai-toyo-sport@tcct.zaq.ne.jp　：事業団
- zai-toyo-sport_g.a.s@mail.zaq.jp　：総務課
- 各体育施設設定@mail.zaq.jp　：各施設
- 個人名(名_性)@toyosport.onmicrosoft.com：個人

■メールの私的利用は禁止する。
■フリーメールアドレス及びフリーメールソフトの使用は禁止する。
■メールアドレス帳に、業務以外のメールアドレスを保存しない。
■件名を不明確な状態で送付しない。『(例）○○　様　「△△△△△の件」』
■施設宛や職員宛に送信された公的メールを許可なく他人のメールアドレスに送信することは禁止する。
■送信時には、その対象によって、下記の表のとおり、『C.C』をつけて送信する。
■自分宛てに届いたメールは送信者が許可していない限り他人には見せない。
■自分のところへ『他の人宛のメール』が間違って届いた場合は、内容は読まずに破棄する。
■自分宛以外の不明な送信者メールを開封せず、破棄する。
■不明な添付ファイルを開封してはならない。
■プレビュー画面を表示しない設定にすること。
■メールの転送先を、個人の使用するメールアドレスに設定しない。
■送信対象者が限定されており、メーリングリストがある場合は、メーリングリストを利用すること。個々人のアドレスをピックアップして、送付しない。
■業務連絡において、所属長・施設長が受信したメールは、転送を限定されたものを除き、速やかに課または施設内職員に通知すること。

公表範囲	市民・対外・業者	各施設との連絡	職員個人
事業団 zai-toyo-sport@tcct.zaq.ne.jp	◎	◎	◎(C.C) [施設長]
総務課 zai-toyo-sport_g.a.s@mail.zaq.jp	◎	◎(C.C) [所属長]	◎(C.C) [施設長]
各施設 各体育施設設定@mail.zaq.jp	◎	◎(C.C) [施設長・所属長]	◎(C.C) [施設長]
事業団職員 個人名@toyosport.onmicrosoft.com	△※	◎(C.C) [施設長・所属長]	◎(C.C) [施設長]

※「事業団職員（個人)」が「市民・対外業者」にメールを使用は原則禁止である。ただし、業務の円滑な連絡手段として使用する場合、所属長もしくは施設長に申請し許可を受け行う。
所属長または施設長は、許可した旨を保護管理者へ報告する。

（19）労働組合及び労働者代表のメールの使用

【運用及びその規定】

① メールアドレスおよびパスワードに関して

1. メールアドレスの使用
   労働組合…下記アドレス(a)を、組合役員で共通使用する。
   各施設労働者代表…下記アドレス(b～i)を使用する。

	所属	メールアドレス	
a	労働組合	union@toyosport.onmicrosoft.com	未使用
b	事務局	jimu_rep@toyosport.onmicrosoft.com	使用中
c	二ノ切温水プール	ninokiri_p_rep@toyosport.onmicrosoft.com	使用中
d	豊島温水プール	teshima_p_rep@toyosport.onmicrosoft.com	使用中
e	武道館ひびき	budou_rep@toyosport.onmicrosoft.com	未使用
f	豊島体育館	teshima_rep@toyosport.onmicrosoft.com	未使用
g	柴原体育館	shibahara_rep@toyosport.onmicrosoft.com	未使用
h	庄内体育館	syounai_rep@toyosport.onmicrosoft.com	未使用
i	千里体育館	senri_rep@toyosport.onmicrosoft.com	未使用

2. パスワードの管理
   変更サイクルは、現行の Office365 下における管理と同様とする(90 日間)
   労働組合…代表にて設定する(ログ切り替えにより使用)
   各施設労働者代表…代表にて設定する(ログ切り替えにより使用)

② メールアカウント使用における遵守(禁止) 事項について。

1. 労働組合、各館労働者代表、それぞれのメールアカウントについては総務課、労働組合、各館労働者代表間での使用のみとし、またこのアドレスを使用しての職員(プロパー、任期付職員、時短職員、非常勤職員) への連絡など、当該目的以外の使用は禁止する。
2. メールの送信の際には、総務課課長あて C.C.の添付を必須とする。
3. 情報保護に関しては情報セキュリティ対策基準(当マニュアル)に準ずる。
4. 個人情報に関するやり取りは禁止する。
5. 情報通信機器の使用については、財団からその業務の用途として貸与している情報通信機器のみとし、それ以外の全ての情報発信機器(私物情報通信機器：スマートフォン、タブレット端末などの携帯端末を含む)を介しての送受信及び閲覧は禁止する。
6. 前項全てにおける、不備、不正などが発覚した場合、情報管理権限者の管理の下、即時に当該ユーザーのメールアカウントを使用禁止とし、場合によってはその削除も行い、その後その旨当該ユーザーに通知し、それ以降メールアカウントの貸与及び使用を禁止する。

（20）マイナンバーの運用について

【総則】
マイナンバーの保管、運用、破棄についての所管課は総務課とし、総務課長を長としたセキュリティ体制を確立する。

【収集・保管・運用・破棄について】
① 収集について
マイナンバー収取担当者において、通知カード(コピー)もしくはマイナンバー付き住民票の提出により収集を行い、本人確認については免許証(コピー)、パスポート(コピー)もしくは年金手帳+保険証の組み合わせのコピーを以て本人確認を行う。
提出分の通知カードのコピーについては財団内各施設でのコピー機は使用せず、当人にて行ったコピーのみを提出する。

② 保管について
収集したマイナンバーについては紙媒体・電子記録の 2 種類を以て保管する。
上記した 2 種の保管方法については、金庫及び鍵付書棚にそれぞれ分けて行うものとする。
金庫及び書棚の鍵については総務課長の命を受けた担当者(以下：担当者)が管理するものとする。

③ 運用について
総務課給与計算用 PC にてのみ入力使用とする。
他の一切の PC ではマイナンバーの入力・使用は行わない。
総務課給与計算用 PC でマイナンバーを取り扱う際には USB メモリー型符号により分割されたデータを合致させ使用する(PC 単独では使用不可)
USB メモリー型符号については 2 本用意し、1 本は金庫にて保管し、他の 1 本は担当者が管理するものとする。

④ 破棄について
総務課給与計算用 PC にて退職処理をされたものについては、7 年後の該当月に破棄予定のお知らせが掲示されるので、紙媒体・電子媒体共に適正処置にて破棄を行う。

【セキュリティ体制について】
紙媒体以外にはすべてアクセスに関して暗号化もしくは使用に関しての「鍵」を必要とするシステムにて運用を行う。

【情報の取り扱い区域に関して】
総務課給与計算用 PC については他の職員による覗き見などが起こらない様に配置する。

附　　則

この対策基準は、平成 24 年 7 月 1 日から施行する。

附　　則

この対策基準は、平成 24 年 9 月 1 日から施行する。

附　　則

この対策基準は、平成 25 年 2 月 1 日から施行する。

附　　則

この対策基準は、平成 26 年 4 月 1 日から施行する。

附　　則

この対策基準は、平成 26 年 11 月 1 日から施行する。

附　　則

この対策基準は、平成 28 年 1 月 1 日から施行する。