

DATA PROTECTION & CYBERCRIME MANUAL (2024)



DATA PROTECTION & CYBERCRIME MANUAL (2024)

REGULATIONS GOVERNING DATA PROTECTION & CYBERCRIMES

This manual was first drafted and technically vetted by the Information Technology and Legal Advisors on the 31st day of December 2024 as the legal authority governing data protection and cybercrimes for the Association.

Signed by: _____

Krislin Goulbourne-Harry
Information Technology Advisor

Date: 31/12/2024

Signed by: _____

Rennie Miller
Legal Advisor

Date: 31/12/2024

DATA PROTECTION & CYBERCRIME MANUAL (2024)

PREAMBLE

As a non-profitable organisation incorporated under the Companies Act of Jamaica, we aim to be proactive in preserving privacy, personal data and counterattack acts of cybercrimes. The Association therefore adopts this manual as its regulatory guideline governing data protection and cybercrime. This regulation hereafter will be called: "DPCM 01/2024".

The guidelines in the DPCM 01/2016 cover law of Jamaica dealing with: (i) Cybercrimes, (ii) Intellectual Property Rights, (iii) Criminal Justice Act, (iv) MOCA Act, (v) JIPO Regulations, (vi) Proceeds of Crime Act, (vii) Law Reform (Fraudulent Transaction), (viii) Data Protection Act and (ix) the Association's Constitution.

The laws are expected to be followed in its entirety given the technological and litigating era live in. The Association has taken the necessary steps to protect any subject relating to data privacy protect, personal protection and intellectual property protection.

VISION

This manual is drafted with the vision of helping the Denbigh High School Past Students Association to bolster its legal framework pursuant to Article 10 section (9)(d) [Constitution modified 2024]. The mission isn't just limited to the wording of Article 9 section (9)(d) but also to hacking of website, social media platforms, misrepresentation, cyber embezzlement, encroachment of intellectual property rights, confidential information, and safeguarding data.

MISSION

The DPCM will serve as a blueprint for the Association members to help protecting against all cybercrimes, setting up a resilient system to vanguard the effective and corrective measures to protect data security and/or privacy, confidential information and intellectual property protection.

DATA PROTECTION & CYBERCRIME MANUAL (2024)

REGULATION 1. CYBERCRIMES

1.1: Cybercrime for the purpose of this manual is defined as any criminal activity that is carried out using digital gadgets and/or digital networks.

1.2: DIGITAL GADGETS

Digital gadgets are deemed as any technological device used to perpetrate a felonious act such as but not limited to:

- (i) Computer;
- (ii) Smartphones;
- (iii) Tablet;
- (iv) Smart glasses and watches;
- (v) streaming devices;
- (vi) Gaming Consoles;
- (vii) Laptops;
- (viii) Digital cameras;
- (ix) Fitness tracker;
- (x) GPS;
- (xi) Input devices;
- (xii) Smart TV;
- (xiii) Any messenger app; and
- (xiv) Any other gadgets or paraphernalia that can be used to insert, receive and/or store data and/or information digitally.

1.3: SMARTPHONE/ PARAPHENALIA

1.3.1: A smartphone and/or paraphernalia is a gadget that:

- (a) has internet function and compatibility;
- (b) has camera, Bluetooth, infrared amongst any other technological device that can be used to transfer or disseminate data from device to another to another via the internet).

1.3.2: For the purpose of this manual an ordinary cell phone can be categorised in this definition once it has the compatibility to transfer, received and/or place data via the internet.

DATA PROTECTION & CYBERCRIME MANUAL (2024)

1.4: CYBER HARASSMENT

1.4.1: Cyber harassment is deemed as circulating erroneous, defamatory, threatening, disparaging, insulting, hurting and malicious information placed on the Association website, social media platforms; and/or text messages, voicemails, pictures and emails sent to any cell phone belonging to the Association.

1.4.2: Cyber harassment is not deemed unconstitutional if it is information done under free speech protection.

1.4.3: Sufficing to say, if the opinion (free speech) even though it is protected under Jamaica's Constitution [Chapter 13, modified 2012] should be placed on the Association's website, social media platforms and/or cell phone with malice aforethought, such an act will render the protection null and void if authorisation is not given to the Executive Committee and consent is not granted to place it on any if the gadget above mentioned.

1.4.5: Cybercrimes will be governed under the Jamaica Cybercrimes Act [2015].

REGULATION 2: CONFIDENTIAL INFORMATION

2.1: Confidential information is any private and/or privilege information surrounding the Association's operation but not limited to:

- (a) Minutes of meetings;
- (b) Informal and formal discussions whether it be orally or written touching and/or concerning the operation of the Association;
- (c) Subcommittee meetings;
- (d) Bank information including Personal Identification Number (PIN); signatures of signatories on the account and financial records;
- (e) Personal privacy such as TRN of the Association Executive Committee Members; home address; workplace and other information regarding to personal privacy;
- (f) Trade secret;
- (g) Marketing strategies; and
- (h) Divulging Social Media Platforms passwords and/or Codes to any unauthorised person.

2.2: Confidential information is categorised as any privileged information albeit it in written or oral communication and/or data which should only be accessible to the Association Executives and its relevant subcommittees, that is deemed strictly confidential and confidential to the receiving member from the disclosing emitter.

DATA PROTECTION & CYBERCRIME MANUAL (2024)

2.3: Confidential information breach will be a misdemeanour which requires a vote of confidence against an office holder or depending on the gravity of the breach of confidence, the Disciplinary Committee of the Association will apply the relevant law to the misdemeanour.

2.4: Confidential information falls under copyright protection and as such infringement thereto will result in sanction back by law and/or the Association's Constitution.

2.5: Confidential information will be governed by (i) JIPO's regulations, (ii) Copyright Act [2015], (iii) Copyright Act [Amendment 2023], (iv) Copyright regulations, (v) Trademarks (Amendment) Acts 2013 & 2021.

REGULATION 3: INTELLECTUAL PROPERTY RIGHTS

3.1: Intellectual Property Rights are any creation of the mind invented by the Association in any of the categories below: (a) Copyright; (b) Confidential Information (Breach of Confidence); (c) Trademarks; and (d) Patents.

3.2: COPYRIGHT

3.2.1: Copyright includes any of the criteria below:

(a) Original literary; (b) Artistic work; (b) Dramatic work; (c) Musical work; (d) Sound recording; and (e) Videoing (live streaming and/or recorded streaming).

3.3: LITERARY WORK

3.3.1: This embodies any work other than musical that is written spoken or sung by the Association such as:

(a) Minutes of meetings and Newsletters; (b) Computer programmes; (c) Lyrics; and (d) Any conferences, AGM and and/or unction which spoken production will be done.

3.4: ARTISTIC WORK

3.4.1: This includes any of the pointers enumerated hereunder:

(a) Graphic; (b) Lithograph; (c) Photographs; (d) Collages; (e) Sculptures; (f) Paintings; (g) Engraving; and (h) Maps, Charts, and Plans.

DATA PROTECTION & CYBERCRIME MANUAL (2024)

3.5: The exception to Copyright protection under the Copyright Act [1993] are:

(a) Titles by themselves; (b) Names; (c) Short phrases; (d) Slogans; (e) Factual information; (f) Concepts; (g) Principles; (h) Processes; (i) Method; and (j) Procedure.

3.6: TRADE MARK

3.6.1: According to the Trade Mark [1999] a trademark is defined as a sign that is capable of being graphically represented and capable of distinguishing the goods or services of one undertaking from those of another undertaking. Moral rights are non-transferrable; thus, this remains the sole property of the Association.

3.6.2: A Sign includes: (a) A word, such as personal name; (b) A design; (c) A letter; (d) A numeral; (e) A colour and/or combination of colours; and (f) Shape of goods.

3.6.3: Any trademark that the Association develops will be registered which gives autonomy to the Association to have exclusive proprietorship in such a trademark.

3.6.4: Registered trademark will be used as a promoting tool for the Denbigh High School PSA services and goods which it offers.

3.6.5: Any patent invention by the Association will follow the stricture under section 4(1) Patent and Design Act [2020].

3.6.7: Information on the social media platforms and website of the Association cannot be retrieved and /or downloaded for commercial and malicious purposes. Authorisation should be granted at all times should a member want to download, store and/or use any IP protected information.

3.6.8: Attribution has to be done for intellectual property rights if a user wants to download or used the information for research and educational purposes.

3.6.9: Documents, information and data cannot be modified without written consent from the Association's Executive Committee which a vote will take place.

3.7: Moral rights remains the sole property of the Association.

3.8: Passing off of any intellectual property accrued, amassed, created, obtained or bequeathed is intellectual property infringement.

REGULATION 4: DATA PROTECTION

4.1: Data Protection is the medium for protecting sensitive and confidential information from being compromised and/or damaged, corrupted and loss.

DATA PROTECTION & CYBERCRIME MANUAL (2024)

4.2: Data privacy is intended to protect the Association's intellectual property rights which confers ownership and cybersecurity to data creative work.

4.3: Passwords; encryption codes and keys; algorithms; software; data masking; authentication; backups; access control; tokenisation inter alia; should not be shared with anyone other than the authorised personnel and the Information Technology Advisor.

4.4: To safeguard data protection, the Association through its IT advisor shall implement the following measures: (I) Data security protection; (ii) Encrypted sensitive data and/or information that unauthorised persons cannot read; (iii) Cybersecurity albeit traditional security and/or AI security; (iv) Data discovery, data loss prevention; and (b) Data risk assessment.

4.5: No modification and or insertion on content and image on the Association's website and Social Media pages should be done without written communication to the IT Advisor and or Social Media Manager who will share the content with the legal counsel and executive members for approval.

4.6: The IT advisor has the authority to suspend any social media account and temporarily shut down the website to bar disinformation, disparaging and insulting information placed online which can harm the Association.

4.7: The IT advisor will be totally immune from litigation once he or she is acting according to the powers vested here and pursuant to Article IX section 9 of the Constitution.

4.8: The IT advisor should act in good faith of the Constitution failure to which immunity will be null and void and should malicious and intentional tactics be used to sabotage access, storage and usage of data of the website and social media pages then due diligence will proceed and the sanctions enshrined under the Constitution will be applied accordingly.

4.9: Any unauthorised posting, cloning, hacking and manipulation of the Association's website and social media platforms will be deemed illegal and the full force of the constitution will be applied should such be discoverable.

4.10: The Data Protection Act [2020] will be the authoritative document should gross violations of data privacy is breach and litigation should ensue.

4.11: Sections 5 must be respected at all times: "Private Information of minor and disable members who are unable to act cannot be accessed or placed on any of the Association's print, digital and analogues without the consent of either parents for minors and legal guardian for the mental or disable".

4.12: Section 6 - The IT advisor is bound by law to provide access to data or information once it is required by legal or lawful demands pursuant to section 8(i) and such should be done within 30 days.

DATA PROTECTION & CYBERCRIME MANUAL (2024)

4.13: The legal advisor will guide the Association as per legal requirements governing request to data pursuant to section 6 and 8(i) as a duty of care is incumbent on the Association.

4.14: Section 21 - Standard of data protection will be adhered to at all time as per DPA [2020].

4.15: Section 30 - subsection 7 will be actionable should a member and or any unauthorised person breach the Association's data manual.

4.16: All other section relevant under the Data Protection Act [2020] will be triggered once infringement is found by its members, third party and/or officers.

REGULATION 5: MISREPRESENTATION

5.1: Misrepresentation for the purpose of this manual is any act, false information and material which misleads an entity or a person to solicit information or funding on the Association's behalf.

5.2: Any request for money, sponsorship and benefit for the Association has to come through the Financial and Fund-Raising Committee.

5.3: The requisition underpinned under the Law Reform (FRAUDULENT TRANSACTIONS) L.N128/2016, the Proceed of Crimes Act [2007], modified 2016, Jamaica Criminal Justice Act [2014], Cybercrimes Act [2015] and MOCA [2018], will take effect if any Association member, officer and any unauthorised person commits an offence.

REGULATION 6: HACKING

6.1: Hacking is defined as manipulation and accessing data unauthorised data in a system or computer.

6.2: Data hacking will be governed under the Data Protection Act [2020] and the Law Reform (Fraudulent Transactions) L.N 128/2016 and the Cybercrimes Act [2015].

REGULATION 7: PHISHING

7.1: Phishing is the practice of sending fraudulent and or misleading information under the disguise of the Association and its Executive Members through email and SMS message.

7.2: No email and SMS messages will be sent to any member of the Executive Committee without it be sent in the executive WhatsApp group.

7.3: Any suspicious email and text message(s) which embodies the semblance of phishing will be legally vetted before responding to said.

DATA PROTECTION & CYBERCRIME MANUAL (2024)

7.4: Email address or addresses of any individual who engages in phishing will be blocked instantaneously, at no time the Association will ask you for your bank, debit and credit card information.

7.5: If you receive any such email and or text message, please email or message the Denbigh High School PSA who will communicate with you directly via an emergency executive meeting.

COMPLIANCE ADDENDUM

The following provisions are formally inserted into this manual as mandatory compliance pointers required to operationalise corporate communication guidelines and ensure alignment with the Jamaica Data Protection Act (DPA), 2020.

REGULATION 7A: CORPORATE EMAIL & ELECTRONIC COMMUNICATION POLICY

7A.1: AUTHORISED USE OF ALUMNI CONTACT LISTS

The Association's past student email database is classified as strictly Confidential Information under Regulation 2.

- (a) The database shall never be shared, traded, or distributed to individual members, third-party entities, or political campaigns.
- (b) Mass electronic broadcasts shall be dispatched exclusively through the Association's authorised marketing platform as managed by the IT Administrator (Advisor).

7A.2: MANDATORY BLIND CARBON COPY (BCC) PRIVACY RULE

In the event that an Executive Committee member or subcommittee chair must send an official operational email to multiple alumni using a standard email client (e.g., Gmail, Outlook), they are strictly required to use the Blind Carbon Copy (BCC) field for all recipient addresses.

- (a) Exposing the personal email addresses of past students in the 'To' or 'CC' fields to other recipients constitutes a formal Data Privacy Breach under Regulation 4.

7A.3: RETIREMENT OF PERSONAL EMAIL CLIENTS FOR ADMINISTRATIVE BUSINESS

All official correspondences concerning the administrative decisions, financial accounts, or legal matters of the Association must be conducted using official domain-specific email addresses (e.g., secretary@denbighhighpsa.org) provided by the IT team.

DATA PROTECTION & CYBERCRIME MANUAL (2024)

(a) The use of personal email addresses (e.g., @gmail.com) to store, transmit, or process sensitive past student data or bank details is prohibited.

7A.4: RETENTION AND DATA PURGING

In accordance with the Data Retention principles of Jamaica's Data Protection Act 2020, any email correspondence containing sensitive member attributes or financial records must be safely purged or permanently encrypted after seven (7) years of inactivity, or upon the formal erasure request of a member.

7A.5: ENFORCEMENT AND SANCTIONS

Any deliberate or grossly negligent violation of this Email Policy shall instantly trigger an executive review under Regulation 2.3. The Disciplinary Committee shall enforce penalties up to and including a vote of no confidence, removal from executive office, or suspension of association membership privileges.

REGULATION 8: STATUTORY DATA PROTECTION PRINCIPLES

Pursuant to the DPA 2020, the Association explicitly adopts the statutory principles of data handling, mandating that all processing of past student information must be executed with fair and lawful justification, restricted to stated alumni purposes, limited to data minimization, and protected by updated security mechanisms overseen by the technical administration.

REGULATION 9: FORMALISATION OF THE DATA PROTECTION OFFICER (DPO)

The Association's Information Technology Advisor is hereby designated with the administrative authority of the Data Protection Officer (DPO). The IT Advisor will monitor internal registries, manage statutory data tracking sheets, and serve as the formal compliance bridge to the Office of the Information Commissioner (OIC), Jamaica.

REGULATION 10: ALUMNI DATA SUBJECT RIGHTS

All registered past students possess enforceable rights regarding their information under Jamaican law. The Association guarantees the Right of Access to files, the Right to Rectification

DATA PROTECTION & CYBERCRIME MANUAL (2024)

of typos, and the absolute 'Right to be Forgotten' (permanent data deletion) upon a member's formal written request, which must be fulfilled within the legal 30-day window.

REGULATION 11: VENDOR MANAGEMENT & CROSS-BORDER TRANSFERS

Any third-party digital tools used by the Association (e.g., mass-mailing systems, website registration portals, or secure dues payment gateways) must contractually comply with local

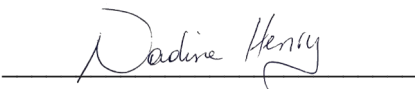
data protection standard policies. Secure encryption must safeguard any information processed across international borders to support diaspora chapters (USA, Canada, UK).

REGULATION 12: DATA BREACH NOTIFICATION PROTOCOL

In the event of an archive leak or unauthorised data breach, the IT Advisor must activate a step-by-step reporting lifecycle. The Association is legally bound to notify the Office of the Information Commissioner (OIC) and all affected alumni within the strict statutory timeframes required by the DPA 2020.

LEADERSHIP TRIPLE SIGN-OFF AND ADOPTION

By signing below, the executive officers confirm that this document represents the approved regulatory authority governing data protection, electronic communication rules, and cybercrime controls for the Denbigh High School Past Students' Association.



Nadine Henry

Association Executive President

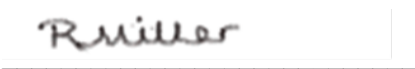
Date: 31/12/2024



Krislin Goulbourne-Harry

Information Technology Advisor

Date: 31/12/2024



Rennie Miller

Legal Advisor

Date: 31/12/2024

DATA PROTECTION & CYBERCRIME MANUAL (2024)