THE NEWMAN CATHOLIC COLLEGIATE

Information Security Policy

Approved by:		**Date:**	18.01.2019
Last reviewed on:			
Next review due by:	31.01.2021		

1. Introduction

1.1 Information is one of the collegiate's most important assets. Failure to ensure adequate security and protection of information held by the collegiate and its associated academies may lead to legal action against the collegiate and/or the individual responsible for the breach. Such legal action could include an investigation by the Information Commissioner's Office ("ICO") who can impose significant financial penalties and/or a claim for damages for breach of the General Data Protection Regulation and the Data Protection Act 2018 (together the "Data Protection Legislation").

1.2 In addition to the possibility of legal action being taken against the collegiate, if the information held by the collegiate and its associated academies is not kept safe, confidence in the collegiate and its associated academies by pupils, parents, guardians, volunteers, the Board of Governors, members of staff and the public at large could be irreparably damaged.

1.3 Keeping information secure yet available to those that need it often presents a difficult challenge. This policy strives to achieve a sensible balance of securing the information held by the collegiate while making it accessible to those who need the information. The collegiate will always however favour security over accessibility where there is any doubt as to the security of information.

2. Definitions

2.1 The Collegiate means The Newman Catholic Collegiate and its associated academies.

2.2 Data means Personal Data and Special Category Personal Data.

2.3 Data Controller is the person who or the organisation which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation.

2.4 Data Subject means all living individuals about whom the collegiate holds Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in respect of their Data and the information that the collegiate holds about them.

2.5 Data Processor means any person who or organisation which processes Data on behalf of the Data Controller including contractors, and suppliers and any third party whose work involves accessing or otherwise using Data held by the collegiate. Data Processors have a duty to protect the information they process for and on behalf of the collegiate by following this and other collegiate information governance policies at all times. "Data Protection Legislation" means the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

2.6 Information Asset means Data held by the collegiate in any form. This Data may be held electronically by software in computer systems and transferred across a network, on paper, in files or transferred by post, courier or in person;

2.7 Information Governance Policy means the General Data Protection Policy, Information Security, Retention, Disposal and Records Management policies and any other policies which may from time to time be in place at the collegiate;

2.8 ICO means the Information Commissioner's Office.

2.9 Information Security means the protection of information and information systems against unauthorised access to or modification of information, whether in electronic or manual storage, Processing, transit and against the denial of service to authorised users.

2.10 Information Security Breach means a breach which may be caused by a technical failure, unauthorised access to either the collegiate networks or a Personal Device used for collegiate business by a third party, loss of the collegiate's information and/or inappropriate actions of an individual or individuals which result in the compromise of information belonging to or held by the collegiate.

2.11 Information Security Vulnerability means an identified weakness of a system(s) or process that puts the security and availability of information at risk.

2.12 Member of Staff means individuals working at the collegiate whether on a full time, part time, temporary, fixed term, casual or volunteer basis.

2.13 Personal Device means the use of laptops, tablets, smartphones or other personal computer equipment used for the carrying out of collegiate business or the processing or storing of information.

2.14 Personal Data means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.15 Processing means any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, erasure or destruction. Processing also includes transferring personal data to third parties.

2.16 Removable Media includes USB sticks, external hard drives, CD's or other media which can be connected to the collegiate networks or a Personal Device and used for storing information.

2.17 Special Category Personal Data means information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.

2.18 Social Media means websites and applications that enable users to create and share content or to participate in social networking including Facebook, LinkedIn, Twitter, Google+, and all other social networking sites, internet postings and blogs. It applies to use of Social Media for collegiate purposes as well as personal use that may affect the collegiate in any way.

2.19 Subject Access Request ("SAR") means a request by an individual to the collegiate pursuant to Article 15 of the GDPR.

2.20 Cloud service/ Cloud computing service is the delivery of computing resources using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local servers or a personal computer.

3. Summary

3.1 Much of the information held by the collegiate is confidential and sensitive in nature. Therefore it is necessary for all information systems to have appropriate protection against adverse events (accidental or malicious) which may put at risk the activities of the collegiate or protection of the information held.

3.2 The collegiate has a responsibility to maintain:

- **Confidentiality** – access to Data must be confined to those with specific authority to view the Data in question;

- **Integrity** – information should be complete and accurate. All systems, assets and applicable networks must operate correctly and according to any designated specification;

- **Availability** – information must be available and delivered to the right person at the time when it is needed and in accordance with the relevant statutory provisions.

3.3 The collegiate must minimise the risk of data security breaches and any person connected to or acting on behalf of the collegiate must meet the minimum requirements as set by the collegiate for connecting to any network operated by or on behalf of the collegiate. This can be found in Appendix 1.

3.4 It is important that members of staff, governors or anyone else acting on behalf or with the authority of the collegiate:

a. Are aware of how and under what circumstances they are permitted to access Personal Data held by or on behalf of the collegiate.
b. Is aware of who they are allowed to share Personal Data and other information with and how it can and should be shared.
c. Reports any Information Security incidents/breaches including phishing emails to the Data Protection Officer in respect of information held by the collegiate.
d. Ensures Data is stored and handled securely and in accordance with this and the other information governance and IT Policies.

e. Does not ignore, turn off or otherwise bypass any Information Security controls put in place by the collegiate.
f. Does not send, distribute or otherwise divulge Data unless permitted to do so. The sending or distribution of any Data should only be done in accordance with the applicable statutory provisions, this policy and any other applicable policy of the collegiate.
g. Data should only be sent by secure methods and, where necessary, should be encrypted/password protected.

4. Policy Statement

4.1 It is essential that the collegiate information systems and data networks are adequately protected from events which may compromise the information held or the carrying on of collegiate business and to this end the collegiate is committed to developing and maintaining an information systems structure which has an appropriate level of security.

4.2 The collegiate will maintain the security and confidentiality of Data held by it, its information security systems and relevant applications and networks for which it is directly responsible by:

a. Ensuring appropriate technical and organisational measures are in place to prevent unauthorised access, damage or interference to and/or with information, IT assets and network services;

b. Ensuring that it is aware of, and complies with, the relevant legislation as described in this and the other information governance and IT Policies;

c. Describing the principles of Information Security to members of staff, pupils, governors and volunteers and explaining how they will be implemented by the collegiate;

d. Protecting Data and other information held by and/or on behalf of the collegiate.

4.3 To ensure a consistent approach to Information Security, the controls set out at paragraphs 7 and 8 of this policy will apply.

5. Use of Personal Devices

5.1 Before using a Personal Device for, or in connection with collegiate business, users must read and sign the Personal Devices Statement.

5.2 Personal Devices used for, or in connection with, collegiate business and in particular for the collection or storing of Personal Data and/or Special Category Personal Data must be kept secure with complex passwords containing a combination of capital letters, numbers and symbols;

5.3 Personal Devices used for, or in connection with, collegiate business should be kept secure at all times and be protected against loss, damage, misuse or unauthorised access.

5.4 The use of Personal Devices in public for, or in connection with, collegiate business should be kept to a minimum to reduce the risk of unauthorised access to Personal Data or Special Category Personal Data.

5.5 Personal Devices used for, or in connection with, collegiate business must have antivirus software installed and be updated with the manufacturer’s software and other updates regularly when updates become available.

5.6 If a Personal Device used for, or in connection with collegiate business is lost or stolen, the loss/theft should be reported to collegiate Business Director, IT Support Team and Data Protection Officer immediately. Where possible the Personal Device should be remotely accessed and the information erased.

6. Removable Media

6.1 Only Removable Media provided by the collegiate that has been encrypted should be used for the storing of Personal Data or Special Category Personal Data.

6.2 Removable Media should be stored securely.

7. Securing Information

7.1 **Physical Access Controls**

a. A nominated member of the collegiate will be responsible for ensuring the Information Security of all Information Assets held by or on behalf of the collegiate. The nominated person/s (usually the Academy Manager) will also have and maintain an Data Asset Register which should record all Information Assets held by the collegiate;

b. A copy of the Data Asset Register will be filed with the Business Director of the collegiate each year.

c. The collegiate will ensure that only authorised individuals are allowed access to restricted areas containing Personal Data or Special Category Personal Data or information systems where there is an identifiable need to access that area;

d. Access to Personal Data and/or restricted areas will be monitored by the nominated person to ensure authorised access to relevant information and to prevent unauthorised access to Personal Data or Special Category Personal Data;

e. Where an unidentified person or any other person without authorisation to be in a restricted area is found, the individual is to be challenged as to their identity and the purpose for which they are in the restricted area. If the unauthorised individual has no legitimate reason to be in the restricted area, this information is to be logged as an Information Security Breach and the Data Protection Officer and Business Director should be consulted as to whether the matter requires reporting to the ICO;

f. External doors and windows must be locked at the end of each day.

g. Equipment that serves multiple users must be capable of identifying and verifying the identity of each authorised user.

h. Members of staff of the collegiate with access to and use of Data must maintain a clear desk and clear screen policy to reduce the risk of unauthorised access to Information Assets such as papers, media and information processing facilities.

i. Personal Devices and computers whether belonging to the collegiate that are used for, or in connection with collegiate business must be switched off or controlled by a complex password (see definitions) when unattended or not in use.

j. Data recorded on paper must be kept locked away in a safe, cabinet or other form of secure furniture when not in use.

k. Confidential information about the collegiate whether stored electronically or on paper must be kept locked away in a secure room or in a safe, cabinet or other form of secure furniture when not in use.

l. Documents containing Data must not be left unattended at printers, photocopiers, scanners or fax machines and must be removed immediately when received.

7.2 **Password and Access Control**

a. Access to Data contained within or accessed from the collegiate and/or academies network(s) will be controlled and restricted to authorised users only;

b. Members of staff of the collegiate who have access to Data are responsible for keeping their own password secure and must ensure their password is neither disclosed to, nor used by, anyone else under any circumstances;

c. Members of staff of the collegiate with access to the collegiate network or a Personal Device used for, or in connection with collegiate business must only access the network or Personal Device using their own login or password;

d. Use of another log in or password will constitute an Information Security Breach and must be reported in accordance with the procedures set out in this policy or any other relevant policy from time to time in force;

7.3 **Cloud Computing**

a. Personal and Special Category Personal Data, whether on the collegiate network or a Personal Device should not be stored on a cloud computing network.

b. If Data or other information concerning or relating to collegiate business is to be stored in or on a cloud network, the collegiate will take all reasonable steps to find out in which country the Data or other information is being stored, and to ensure that appropriate measures are in place in relation to any Data transferred outside of the EEA.

c. If the collegiate receives notification that Data in respect of collegiate business has been corrupted, lost or otherwise compromised while stored on a cloud network, the collegiate should ascertain whether any or all of the information stored in the cloud can be recovered and if this is possible restore that information.

d. Any corruption, loss or compromise of information held on a cloud network should be recorded in the risk register and if appropriate reported via the mandatory reporting procedure set out at paragraph 9 of this Policy.

8. Storing and Transportation of Data

8.1 Data can be vulnerable to loss, unauthorised access, misuse or corruption when being physically transported either personally by members of staff of the collegiate or when sending Data via the postal service or couriers;

8.2 Special controls should be adopted to protect Data from unauthorised disclosure or modification and include:

a. Sending all Special Category Personal Data via secure post such as Royal Mail recorded or signed for delivery or special delivery or as otherwise agreed with the Data Subject;
b. Ensuring the packaging is sufficient to protect the contents from any physical damage likely to arise in transit;
c. Delivering by hand where appropriate;
d. Records containing Special Category Personal Data shall not be delivered by hand unless absolutely necessary. In which case the following should occur:
    1. Documents transported in vehicles should be hidden away or locked in boot where possible.
    2. Documents & mobile devices should never be left unattended even in a locked vehicle.

8.3 Consideration should be given to the necessity of transporting or moving Data or other records as this increases the risk of Data loss.

9. Information Security Incident Reporting and Management

9.1 The collegiate will have and maintain a register where all Data breaches are logged. This log as a minimum should include:

a. The description of the breach;
b. The type of Information affected;
c. How the Information Asset(s) has/have been compromised;
d. Whether any Special Category Personal Data was compromised;
e. Whether the incident needs to be reported in accordance with the mandatory reporting section of this policy at paragraph 9.3 below.

9.2 Where there has been any breach the collegiate Data Protection Officer and Business Director must be informed immediately, so they can decide if an Information Security Breach has occurred and if the DPO should be involved in order that consideration can be given to reporting the breach to the appropriate authorities;

9.3 If there has been an Information Security Breach but it does not require reporting to the ICO, it should be recorded in the Information Security Breach Log see Appendix 2;

9.4 Examples of an Information Security Breach include but are not limited to:

a. Password(s) written down and available by, on or next to a computer or Personal Device used for or in connection with collegiate business;
b. Using another person's password;
c. Divulging of a password;
d. Making use of Personal Data for personal gain;
e. Accessing Data for personal knowledge;
f. Attempting to gain access under false pretences;
g. Unauthorised release of Data;
h. Knowingly entering inaccurate Data;
i. Deleting Data prior to the retention period or any other period set out in the Retention, Disposal and Records Management policy expiring;
j. Loss or misuse of Data;
k. Malicious damage to equipment or Data;
l. Unauthorised removal of Data, collegiate equipment or equipment used for or in connection with collegiate business from collegiate premises or another site authorised for the storage of such information or equipment

10. Business Continuity and Disaster Recovery Plans

10.1 The collegiate has a Business Continuity Plan and each academy has an appendix to this which includes local requirements in the event of interruption caused by a major IT service failure.

10.2 The Collegiate has procedures in place to maintain essential services in the event of an IT system failure.

11. Monitoring and Review

11.1 This policy will be reviewed every two years or earlier if required and may be subject to change

Personal Devices Statement
The collegiate recognises that its employees will use personal devices to access work information and emails. This must be achieved with appropriate protection of the data that is held within the documents. Therefore all Employees using personal devices to access collegiate documents and emails must adhere to the below requirements;

- Personal devices include mobile phones and tablets only.
- Personal Devices used for, or in connection with, collegiate business should be kept secure at all times and be protected against loss, damage, misuse or unauthorised access.
- The use of Personal Devices in public for, or in connection with, collegiate business should be kept to a minimum to reduce the risk of unauthorised access to Personal Data or Special Category Personal Data.
- Personal Devices used for, or in connection with, collegiate business must have antivirus software installed and be updated with the manufacturer's software and other updates regularly when updates become available.

Passwords

- All collegiate data, in particular Personal Data and/or Special Category Personal Data must be kept secure with a complex password.
- If the Personal device is used by numerous people the documents/programmes/emails must not be kept open. They must be accessed through a complex password.
- Personal passwords must not be given to other staff members.

Definition of a complex password: A complex password must contain a combination of capital letters, numbers and symbols.

Lost or Stolen Personal Devices

If a personal device is lost or stolen and has access to collegiate information on it, the following actions must be taken;

a. Contact the Data Protection Officer and IT support immediately, who will assess the risk of loss of data.
b. Immediately remotely access the programme (i.e. emails) and change the password
c. Contact the Business Director or Accounting Officer if there has been a data breach
d. Report to the police or ICO if needed

APPENDIX 1

Minimum security standards for networked client devices

The Newman Catholic Collegiate Information Security Policy requires all network capable devices that connect to any collegiate/collegiate network(s), comply with the following minimum security requirements.
The requirements help to protect both the individual staff member's device and devices connected to the collegiate network(s).
In the event that a staff member's device cannot demonstrate that it meets the minimum requirements, the device must not be connected to the network, unless written authorisation is provided by the Accounting Officer/Principal.

Authentication
Staff member devices must not provide unauthenticated user access. User authentication must be provided by means of complex passphrases or other secure authentication mechanisms.

Unnecessary Software or Services
Devices must not run any software applications or services for any purposes, other than the agreed intended use.

No Unattended User Sessions
Users must not leave the device unattended or locked. The device/operating system should be configured to automatically lock after a defined period of inactivity, or the user must manually suspend or close the active session.

Firewall Software
Staff member devices should be configured to use an active client-based firewall. The firewall software should be configured to only allow incoming traffic for the intended use.

Appendix 2 - Record of Information Security Breaches

Name of Academy -

Date of the Breach	Information Affected	Consequences e.g. who's affected & how	Cause of the breach e.g. human error, IT security	Risk Level – low, medium or high	Action taken to minimise the risk/contain the breach	Actions taken to prevent reoccurrence	Reported to the Police/ICO (if needed)