National Examining Board for Dental Nurses

Policy	**Information Management**
Effective Date	24 July 2018
Scheduled Review Date	July 2021
Supersedes	Information management policy May 2018
Monitored by	Governance Committee
Approved by	Governance Committee on behalf of the Board of Trustees on 23 July 2019

Purpose

This purpose of this policy is to ensure that:

- the confidentiality, security and integrity of personal data held by the organisation is maintained, the data is managed appropriately, and, in a way, which protects individuals' rights
- information related to the organisation's products and services (e.g. examinations) is held confidentially
- information which is needed for organisational and business purposes is managed appropriately and its confidentiality is protected
- the organisation acts lawfully
- the organisation is not exposed to legal, governance, financial or business risks due to the mishandling of information and the organisation's reputation is not adversely affected.

Scope

This policy applies to everyone who works for NEBDN on a paid or unpaid basis. This includes staff, trustees, committee members, examiners, examination teams and suppliers.

Policy statement

As an organisation, NEBDN processes data related to:

- individuals - candidates, course providers and their staff, examiners, helpers, committee members, trustees, suppliers and staff
- the products and services that the organisation offers – examinations, training and development

- the running of the organisation as a charity and a business – accounts, strategic and business plans, policies etc.

The organisation:

1. recognises its responsibilities to protect the confidentiality of personal data – this includes the data of candidates, course providers and their staff, examiners, helpers, committee members, trustees, suppliers and staff
2. recognises its responsibility to treat all candidates for its examinations fairly and hence its need to protect confidential data and information related to this (e.g. question bank items, examination papers)
3. sees well managed information as an organisational asset which is critical to delivering its vision and strategic aims (e.g. the finances of the business, plans for the business, internal organisational discussions about projects and developments)
4. will comply with all relevant statutory and regulatory requirements.

We have identified the current following legal bases for processing personal data:

a. to fulfil the contracts for services that we offer – specifically to candidates and course providers but also in relation to our employees and suppliers
b. the consent of individuals to process their data for specific purpose – this relates to our work with examiners and helpers as well as those who agree that we can send them further information about our products and services (e.g. following trade shows) as well as those who consent to other aspects of our work (e.g. appearing in photos for marketing purposes)
c. to comply with our legal obligations
d. as part of our public duty to protect the public and patients – this relates to the requirements placed upon us when to inform the GDC of any student fitness to practise cases.

As an organisation we use the following general principles of confidentiality:

1. information held by the organisation is assumed to be confidential unless it is in the public domain (i.e. appears on the NEBDN website or in its publications or open correspondence)
2. information is not disclosed to third parties without the consent of the individuals, committees or organisation concerned
3. information is only shared with individuals when appropriate and once thorough checks have been made that the individuals concerned have a right to receive it
4. only the minimum amount that is needed for the purpose is shared

5. as far as is possible, data is anonymised and provided on a group basis so that it is not traceable back to individuals
6. disclosure to a third party is only made when a legal requirement.

A table recording the personal data that we process is at Appendix 1.

A summary of Confidentiality Dos and Don'ts can be found at Appendix 2.

The organisation requires that everyone who processes personal data will comply with the enforceable principles of good practice. These are that personal data, whether paper based or electronic, must be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (further processing for archiving purposes is not included in this)
c. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
d. accurate and where necessary kept up-to-date with every reasonable step being taken to ensure that any inaccurate data is erased or rectified without delay
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The organisation will ensure that:

a. everyone processing personal information is appropriately trained to do so and appropriately supervised
b. any enquiries about handling personal information are dealt with promptly and courteously
c. an individual who wishes to view the information held on them personally can, upon receipt of a subject access request, receive this information in a timely fashion
d. any errors in the data held on an individual are corrected immediately once the organisation becomes aware of the error
e. its processing of personal information is clearly described

f. regular reviews and audits the ways in which it holds, processes and uses personal information

g. any individual who considers that this information management policy has not been followed is able to raise the matter easily with an appropriate person

h. any breaches of data security will be promptly reported to the supervisory authorities

i. have a written contract in place with any organisation that processes personal data on our behalf to ensure that there are sufficient guarantees to meet personal data protection requirements.

The process for submitting and dealing with subject access requests is at Appendix 3.

Organisational data

The policy of NEBDN is to:

1. recognise and make the most of our information assets in line with our charitable objects
2. manage information effectively as a strategic asset across the organisation – by providing timely, appropriate, accurate and up-to-date information at the point of need
3. make information available as quickly and easily as possible including giving individuals information on the data that is held on them following a subject access request
4. take appropriate measures to protect information, including personal information, which cannot be shared for reasons of security or privacy
5. assess and manage risks to the confidentiality, quality, integrity and availability of information
6. ensure that the information created, collected and stored is proportionate to organisational and any legislative or regulatory needs and is retained only for as long as it is needed – Appendix 4 sets out the appropriate retention periods for different types of information
7. ensure information is of the appropriate quality and in the appropriate media to support organisational needs
8. create an information management culture where employees and volunteers take personal responsibility for managing information and are fully supported by their managers
9. provide training and support to encourage the adoption of good practice in information management as set out in this policy.

This policy does not form part of any employee's contract of employment and it may be amended at any time.

NEBDN reserves the right to review, amend and update this policy at any time to reflect best practice and to ensure compliance with any changes or amendments made to the General Data Protection Regulation (GDPR), the Data Protection Act or other relevant legislation.

Definitions

General Data Protection Regulation - GDPR (2016) - GDPR governs how organisations handle personal data (i.e. information that can identify an individual). Compliance is required from 25 May 2018 when the GDPR replaces the Data Protection Act 1998.

Personal Data- is any information relating to an identifiable living person who can be directly or indirectly identified by reference to an identifier. This covers a wide range of personal identifies including: (e.g. name, address, postcode, date of birth, personal phone numbers, bank account details, National Insurance numbers, IP addresses, photographs, video recordings, identification number, location data or any other online identifier).

Sensitive personal data - includes: genetic data, biometric data where processed to uniquely identify an individual, data on sexual orientation, political or religious beliefs and health details. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to processing this type of data.

Individual rights - Data subjects (i.e. individuals) have the following rights:

a. the right to be informed – fair processing information (i.e. data held, lawful basis for processing, purpose it is used for, length of time it will be held and how to withdraw consent
b. the right to access – free of charge (unless a request is manifestly unfounded or excessive, particularly if it is repetitive, in which case a reasonable fee can be charged)
c. the right to rectification – if it is inaccurate or incomplete
d. the right to erasure / be forgotten – where there is no compelling reason for its continued processing (not an absolute right and can be denied if data required in relation to a legal claim or in public interest)
e. the right to restrict / block processing
f. the right to data portability – allows data to be moved from one organisation to another for the subject to get a better deal (e.g. bank accounts)
g. the right to object – to processing of their data for purposes other than those that they have agreed to
h. rights related to automated decision-making including profiling (if it is not required for legal purposes).

Data Controller - determines the purposes and means of processing personal data in an organisation. S/he is responsible for and must be able to demonstrate compliance with the principles for processing personal data.

Data Processor – is responsible for processing personal data on behalf of a data controller. The GDPR places specific legal obligations on anyone who processes personal data (e.g. requirements to maintain records of personal data and processing activities) and a legal liability if there is a breach.

Personal data breach – a breach of security leading to the destruction, loss, alteration, unauthorised disclosure or, or access to, personal data.

Lawful collection - An organisation must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned
- be transparent about how it intends to use the data, and give individuals appropriate privacy notices when collecting their personal data
- handle people's personal data only in ways they would reasonably expect, and
- make sure that it, or anyone working for it, does not do anything unlawful with the data.

Privacy notice - A statement that must be given to everyone before their personal information is collected and stored. This should state:

- the purpose or purposes of the intended use of the information
- give details of the principles and practices used in the recording and storing of personal data
- rights of access to their data.

Privacy and Electronic Communications Regulations (PECR) - PECR sits alongside the Data Protection Act and subsequently the GDPR and offers specific privacy rights in relation to electronic communications. It has specific rules on:

- marketing calls, emails, texts and faxes;
- cookies (and similar technologies);
- keeping communications services secure; and
- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

Legal basis for disclosure - Generally the legal basis for disclosure is through an individual providing consent to the information being disclosed. There are however other specific legal requirements when disclosure must be made which are:

- disclosure required by legislation (e.g. the Prevention of Terrorism Act 1989, Terrorism Act 2000, Terrorism Act 2006, Road Traffic Act (RTA) 1988 and Police & Criminal Evidence Act (PACE) 1984
- Court Orders
- disclosure is "in the public interest" (e.g. the Public Interest Disclosure Act 1998).

Information management means: creating, collecting, recording, accessing, processing, using, sharing, reviewing, storing, retaining, protecting and disposing of information.

Information can be held or given in a number of different forms including: verbally, on paper, using CD/DVD, USB sticks, computer file or printout, laptops, tablets, palmtops, mobile phones, digital cameras.

Responsibilities

The Board of Trustees holds ultimate responsibility for this policy.

The Board of Trustees has delegated the management of this policy to the Governance Committee - it has responsibility for ensuring that the objectives of this policy are achieved and ensuring compliance with legislation and Codes of Practice.

Day to day responsibility for the effective operation of this policy is delegated to the Chief Executive, who will ensure:

1. the organisation complies with the requirements of the GDPR and that the appropriate actions are maintained and in good order (e.g. internal records of the organisation's processing activities, up-to-date and just-in-time privacy notices)
2. there is a consistent approach to good information management practice within NEBDN based on the information life cycle – create, store, discover, use, share, review, record, dispose
3. everyone who works for the organisation is aware of their responsibilities for managing information and protecting data as described in this policy
4. everyone who works for the organisation has the necessary time and resources to create and review information within their area of responsibility
5. individuals receive training and development to improve their information management skills, protect confidentiality and increase their understanding of what a data breach consists of and their duty to report this when it happens
6. the appropriate action is taken when individuals breach confidentiality or act in a way that is inconsistent with this policy
7. ICT platforms are fit for the purpose of effective information management within the organisation including:
    a. Reviewing access to IT systems (e.g. firewall settings, malware protection, software updating, precautions for mobile working (phones and laptops), system access, password strengths and regular updating
    b. Encryption (e.g. sending and receiving data, devices, back-ups)
    c. Data loss (e.g. daily back-up, restoring data from back-ups)
    d. Access to hard copy data
    e. Managing sensitive data
8. that disclosures to a third party are only made when there is a legal requirement to do so (see definitions)

9. that the organisation complies with all legal, statutory and good practice guidance requirements.

The Head of Quality and Standards (or, if they are not available or if their involvement could be seen to potentially compromise the investigation), an appropriate other senior manager) will:

1. lead on the organisation's compliance with the GDPR and other data protection areas ensuring that:
   a. all staff are appropriately developed, supported and appraised to understand and carry out their roles effectively
   b. regular audits are undertaken of the organisation's processing activities and appropriate action is taken to remedy any deficiencies
2. establish the data protection fee that the organisation needs to pay to the ICO and ensure that it is paid on an annual basis

3. promptly notify the Information Commissioner's Office (ICO) if there is a data breach which is likely to result in a risk to the rights and freedoms of individuals, and of notifying individuals where a breach is likely to result in a high risk to their rights and freedoms. Guidance on how to assess the risk and a template form and process for notifying the ICO is set out in Appendix 5. At the same time as notifying the ICO, the CEO will alert the Board of Trustees to the breach and provide advice on whether it is also necessary to report the data breach to the Charity Commission. Guidance from the Charity Commission on when to report a breach is set out in Appendix 6.

All managers and team leaders will:

1. take ownership of, and responsibility for, the management of information created and used within their areas of responsibility
2. ensure that information is accurate and fit for purpose
3. ensure that information has appropriate access and security permissions assigned
4. encourage the sharing of information and knowledge through setting a high standard of personal information management that others can emulate
5. include information management in one to one and team meetings with staff and volunteers
6. ensure that newly recruited employees and volunteers receive appropriate induction and training on this policy and its requirements
7. ensure that those for whom they hold line management responsibility follow this policy.

Everyone who works with or has access to information about or held by NEBDN, needs to be aware of their responsibilities for, and act to, maintain confidentiality and preserve information security. This includes contractors, consultants and suppliers.

All staff and volunteers will act in a way that fully complies with this policy. Specifically, everyone who works for the organisation will:

1. complete a Confidentiality Undertaking at the time intervals required for their role (see Appendix 7)
2. ensure that they are always aware of and respect the confidentiality of information they produce, share or receive
3. treat information as an organisational asset
4. take ownership of, and personal responsibility for, the information they create, capture, maintain or dispose of
5. take personal responsibility for their role in the effective management of the information created and used in their work areas (including maintaining a clear desk so that confidential information cannot seen by those not entitled to see it)
6. make information accessible to those who require it to fulfil their duties
7. seek further advice and support if unsure about their responsibilities under this policy
8. alert an appropriate person if and when they have concerns about this policy not being followed appropriately.

Protecting confidentiality is a legal obligation for everyone who undertakes work on behalf of NEBDN whether this is on a paid or unpaid basis. Failure to follow this policy will be considered misconduct and addressed in accordance with the disciplinary policy and process. regarded as serious misconduct and will be dealt with in accordance with the relevant disciplinary policy and procedures. For example, staff may be subject to dismissal, examiners may be dismissed from the Panel of Examiners and trustees may be removed from the Board. Any person who discloses confidential information may be subject to prosecution for wrongful disclosure. Individuals may be held independently and individually liable for any breaches of confidentiality of personal data collected and stored by the organisation.

References

Information Commissioner's Office, 2017, Overview of the General Data Protection Regulation (GDPR)

Information Commissioner's Office, March 2018 (or most up-to-date version), Guide to the GDPR at www.ico.org.uk

Information Commissioner's Office, 2018, Documentation

For registered dental professionals, the GDC's Standards for the Dental Team – link here

NEBDN Complaints policy NEBDN

Social media policy

NEBDN Whistleblowing policy.

Questions

If you have any questions about this policy, please email NEBDN at info@nebdn.org and your enquiry will be directed to the appropriate member of staff.

Appendix 1: Personal data processed by NEBDN

Individual	***Data processed***	***Reason for retention***
Staff	See Staff records policy.	Contractual
Trustees	Name, address, tel no, DOB, NI, Email (personal), references, CV inc. current and previous employment, bank details, next of kin, special categories, photos, other business dealings (via declaration of interest)	Contractual
Examiners	Name, address, tel no, DOB, NI, Email (personal), references, CV inc. current and previous employment, bank details, next of kin, special categories, photos, other business dealings (via declaration of interest), GDC registration number (and potentially copy certificate) Photos - ID badge. Name, address, tel, bank, NI, email	Contractual
Exam Helpers	Name, address, tel no, DOB, NI, Email (personal), references, CV inc. current and previous employment, bank details, next of kin, special categories, photos, other business dealings (via declaration of interest) Work information, GDC reg Photos - ID badge. Name, address, tel, bank, NI, email	Contractual
Exam Candidates	CRF - Name, address, tel, email, DOB, GDC no, and cert Accreditation - Name, address individuals and company, bank details, org or pers, CV, email, tel, website, GDC and Quals	Contractual
Witnesses (RoE/RoC)	tbc	Contractual
Witness Markers	tbc	Contractual

Other individuals who request information about our products and services	Name, address, email, phone number. Gathered at conferences or exhibitions.	In order to provide info on our products and services
etc		

Appendix 2: Confidentiality Dos and Don'ts

Dos

- Take the same care in handling NEBDN's information as you do when handling your own personal information (e.g. bank details).
- Safeguard the confidentiality of all information that you come into contact with unless you know that it is in the public domain (i.e. you can find it on the website).
- Clearly mark if any papers that you produce are confidential (this should be in the header of documents, and in the subject line of any emails).
- Clear your desk at the end of each day, keeping all portable records containing person identifiable or other confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.
- Switch off computers with access to person-identifiable or other confidential information, or put them into a password-protected mode, if you leave your desk for any length of time.
- Ensure that you cannot be overheard when discussing confidential matters.
- Challenge and verify where necessary the identity of any person who is making a request for person-identifiable or other confidential information and ensure they have a need to know.
- Share only the minimum information necessary.
- Transfer person-identifiable or other confidential information securely (i.e. use a secure email account to send confidential information)
- Seek advice if you need to share person-identifiable information without the consent of the identifiable person's consent and record the decision and any action taken.
- Report any actual or suspected breaches of confidentiality.
- Participate in induction, training and awareness raising sessions on confidentiality issues.

Don'ts

- Don't share passwords or leave them lying around for others to see.

- Don't share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.
- Don't use person-identifiable information unless absolutely necessary and anonymise any information where possible.
- Don't collect, hold or process more information than you need, and do not keep it for longer than necessary.
- Don't share information about the business or its future plans unless you know that these are clearly in the public domain.

Appendix 3: Process for submitting and dealing with subject access requests

Individuals have the right to access their personal data and supplementary information held by NEBDN.

Individuals will have the right to obtain:

- confirmation that their data is held and processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice

How to make a subject access request

Any individual who wishes to view the information held on them personally by NEBDN can make a subject access request. This request must be in writing.

Subject access requests should be sent to:

Email: info@nebdn.org

or

Post: NEBDN
First Floor, Quayside Court
Chain Caul Way
Preston
PR2 2ZP

Subject access requests must include the following information:

- their full name, address, date of birth and contact telephone number
- any information used by NEBDN to identify or distinguish them from others of the same name (e.g. candidate number) if known

- details of the specific information they require and any relevant dates, for example emails between NEBDN and the individual making the request between 1/6/16 and 1/9/17.

How NEBDN will deal with a subject access request

When a subject access request is received by the organisation, the Executive Assistant will acknowledge its receipt to the individual, add the request to a central request log, and use it to monitor progress in dealing with each request. The Executive Assistant will allocate the request to the appropriate team leader or manager at NEBDN Head Office who will take ownership of request.

NEBDN will make information available as quickly and easily as possible. NEBDN will challenge and verify where necessary the identity of any person who is making a request for person-identifiable or other confidential information and ensure they have a right to know.

NEBDN will respond to subject access requests without delay, and at the latest within one month of receipt. However, where requests are complex or numerous, the period may be extended by a further 10 days. If this is the case, NEBDN will explain to the individual why the extension is necessary.

A summary version of the subject access request log will be submitted to each Governance Committee meeting.

Complaints

If you feel that a subject access request has not been dealt with properly as set out in this policy, or if the information that provided to you is inaccurate or unnecessary, you can make a complaint. NEBDN's complaints policy and procedure are available on our website

Appendix 4: Retention periods for different forms of information

Principles

The Data Protection Act 1998 offered useful guidance on the length of time that information should be stored – in short, the time should be adequate, relevant, not excessive, accurate, up to date and not kept for longer than is necessary. Unless the law specifies otherwise, most records can be stored electronically. However due to the risk of obsolescence with electronic records, such records should be retained in at least two formats and anything electronic backed up off site.

Data needs to be stored for the time:

- required by law
- as specified in contracts (e.g. if a funding body has specific requirements)
- as required by the organisation.

Table 1 sets out the requirements for retaining information that are specified in various laws and regulations.

Table 2 sets out NEBDN's organisational requirements for retaining information so that the organisation has the information it needs to manage risk, make effective and efficient decisions and take appropriate actions.

Actions

All NEBDN staff must ensure information and data are retained for the time required by law or by organisational requirements. If in doubt, seek advice before disposing of any document.

Table 1: Legal requirements for retaining data

Information	Period of retention	Reason for retention period
Charity company data		
Trust deeds, governing documents	Permanently	Data Protection Act
Register of members and directors	Permanently	Data Protection Act
Board of trustee's minutes, meetings and decisions	Permanently	Data Protection Act
Annual accounts and annual review	Permanently	Data Protection Act
Major agreements of historical significance	Permanently	Data Protection Act
Investment ledger	Permanently	Companies Act Charities Act
Investment certificates	Permanently	Companies Act

Information	Period of retention	Reason for retention period
		Charities Act
Fixed assets register	Permanently	Companies Act Charities Act
Contracts with customers, suppliers or agents	6 years after the expiry of the contract (or 12 years if contract executed as a deed)	Limitations Act 1980
Insurance and health and safety data		

Health and safety assessments	3 Years for general records Indefinitely for records related to hazardous substances	Personal injury actions must generally be commenced within three years of injury. However industrial injuries not capable of detection within that period (e.g. Asbestos) the time period may be substantially extended.
Accident reports and relevant correspondence	3 years after settlement	Data Protection Act
Employer's Liability Insurance certificate	40 years	Employer's Liability (Compulsory Insurance) Regulations 1998
Insurance policies	3 years after lapse	Data Protection Act
Claims correspondence	3 tears after settlement	Data Protection Act
Financial data		
Purchase invoices • Payments cash book or record of payments made • Purchase ledger • Invoice – revenue • Petty cash records	6 years from the end of the financial year in which the transaction was made	Companies Act Charities Act (HMRC)
Invoice - capital item	10 years	Companies Act Charities Act HMRC
Income / monies received • Bank paying in counterfoils • Bank statements • Remittance advices • Correspondence re donations • Bank reconciliations • Receipts / cash book • Sales ledger	6 years from the end of the financial year in which the transaction was made	Companies Act Charities Act (HMRC)
Deeds of covenant, Gift Aid declarations and legacies	6 years after the last payment made / estate wound up	Data Protection Act
Property leases	15 years after expiry	Limitations Act 1960

Information	Period of retention	Reason for retention period

Payroll documentation • Income tax records – P45 • Notice to employer of tax code (P6) • Annual return of employees and directors' expenses and benefits (P11D) • Certificate of pay and tax deducted (P60) • Notice of tax code change • Annual return of taxable pay and tax deducted • Records of pension deductions • Payroll and payroll control account	6 years + current year	Taxes Management Act Companies Act Charities Act
Pension contributions	Permanently	Companies Act Pensions Act
Employee/personnel data		
Accident Book	3 years after last entry	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995
Personnel files & training records	6 years after employment ceases For senior executives – files should be kept permanently for historical purposes	Limitations Act 1980
Salaries and expenses • Wages and salary records • Expenses accounts / records • Overtime records / authorisation	6 years plus the current year	Taxes Management Act National Minimum Wage Act
Redundancy details, calculations of payments, refunds	6 years after employment ceases	Data Protection Act
Statutory Sick / Maternity Pay records, calculations, certificates	3 years after the end of the tax years in which period ends	Statutory Sick Pay (General) Regulations The Statutory Maternity Pay Regulations
Job application forms & interview notes for unsuccessful candidates	1 year	Equality Act 2008 Limitations Act

Volunteers' records	Full details to be retained for 1 year after volunteer leaves Reduced information relating to dates of volunteering, outline of tasks and any complaints	
Information	**Period of retention**	**Reason for retention period**
	received for 7 years after volunteer leaves	
Records relating to working time	2 years from date on which made	Working Time Regulations

Table 2: Organisational requirements for retaining data

Information	Period of retention
Candidate result records (including personal data to enable candidate identification)	Indefinitely
Fitness to Practice issues	7 years
Course provider records (active provider)	Indefinitely, while active
Course provider records (lapsed provider)	7 years
Complaints	3 years from conclusion
eRoE Witness information	3 years from successful completion of the training program
Team meetings	5 years
Disciplinary Records	2 years – see Disciplinary Policy
Minutes and papers of different meetings	5 years

Any other information kept by staff should be in line with the GDPR and any other legislation and manual and computer records not listed above should be kept for no longer than is necessary in relation to the purpose(s) for which they are held.

Confidential information (including personal data) should be kept securely and disposed of by shredding or a similar method which protects confidentiality.

Appendix 5: Guidance on assessing whether a data breach needs to be reported to the supervising authorities, a template form and process for doing so

A **notifiable** breach of personal data has to be reported to the ICO within 72 hours of the organisation becoming aware of it. It is recognised that it may be impossible to investigate a breach fully within that time-period. The ICO should be provided with as much information as possible in that time period and given more information as it becomes available.

72 hours is a very short timescale within which to determine whether a data breach needs to be reported – at the same time as investigating and taking action to contain the breach – and particularly so if the breach is discovered towards the end of a week. **Urgent action** is required.

How to determine if a breach should be notified to ICO

Although the GDPR introduces the obligation to notify a breach to ICO and to the individuals affected, it is not a requirement to do so in all circumstances:

- notification to the ICO is only triggered where a breach is likely to result in a risk to the rights and freedoms of individuals.
- communication of a breach to the individual is only triggered where it is likely to result in a high risk to their rights and freedoms.

This means that immediately upon becoming aware of a breach, NEBDN should seek to contain and investigate the incident, and assess the risk that could result from it.

Recital 85 of the GDPR explains that:

> "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

When assessing risk, consideration should be given to both the likelihood and severity of the risk to the rights and freedoms of data subjects. Risk exists when the breach may lead to physical, material or non-material damage (e.g. discrimination, identity theft or fraud, financial loss and damage to reputation) for the individuals whose data have been breached. When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur.

The Article 29 WP guidelines (link here) recommend that the assessment of risk takes into account a number of factors. These have been used to create the following template, which should be used to conduct and record the risk assessment, as it is important to have a clear record and audit trail of all decisions about notifying ICO and any individuals whose data has been breached.

Template for assessing whether a breach needs to be notified to ICO

Summary of the breach *(include a summary of what happened, who and what data was involved).*

Factor	*GDPR example, guidance (more detail is at link)*	*NEBDN assessment re this breach*
Definition of breach	Was this "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."? Destruction of personal data is where the data no longer exists, or no longer exists in a form that is of any use to the controller. Damage is where personal data has been altered, corrupted, or is no longer complete. Loss of personal data - the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession. Unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR.	

Factor	*GDPR example, guidance (more detail is at link)*	*NEBDN assessment re this breach*
The type of breach	There are 3 types of breach: 1. Confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, personal data 2. Integrity breach - where there is an unauthorised or accidental alteration of personal data 3. Availability breach - where there is an accidental or unauthorised loss of access to, or destruction of, personal data. Examples of a loss of availability include where data has been deleted either accidentally or by an unauthorised person, or, in the example of securely encrypted data, the decryption key has been lost. In the event that the controller cannot restore access to the data, for example, from a backup, then this is regarded as a permanent loss of availability. A loss of availability may also occur where there has been significant disruption to the normal service of an organisation, for example, experiencing a power failure or denial of service attack, rendering personal data unavailable.	
The nature, sensitivity, and volume of personal data	Breaches involving health data, identity documents, or financial data such as credit card details, can all cause harm on their own, but if used together they could be used for identity theft. A combination of personal data is typically more sensitive than a single piece of personal data. A small amount of highly sensitive personal data can have a high impact on an individual, and a large range of details can reveal a greater range of information about that individual	

Factor	*GDPR example, guidance (more detail is at link)*	*NEBDN assessment re this breach*
Ease of identification of individuals	An important factor to consider is how easy it will be for a party who has access to compromised personal data to identify specific individuals or match the data with other information to identify individuals. Identification may be directly or indirectly possible from the breached data, but it may also depend on the specific context of the breach, and public availability of related personal details. This may be more relevant for confidentiality and availability breaches. Personal data protected by an appropriate level of encryption will be unintelligible to unauthorised persons without the decryption key.	

Factor	*GDPR example, guidance (more detail is at link)*	*NEBDN assessment re this breach*
Severity of consequences for individuals.	Depending on the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. There may be a confidentiality breach, whereby personal data is disclosed to a third party in error, for example, where personal data is sent accidentally to the wrong department of an organisation, or to a commonly used supplier organisation. The controller may request the recipient to either return or securely destroy the data it has received. If the controller has an ongoing relationship with them, and is aware of their procedures, history and other relevant details, the recipient may be considered "trusted", and there may be a level of assurance that the recipient will not to read or access the data sent in error. If this is the case, the fact that the recipient is trusted may reduce the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the supervisory authority, or to the affected individuals.	
Special characteristics of the individual	A breach may affect personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result.	

Factor	*GDPR example, guidance (more detail is at link)*	*NEBDN assessment re this breach*
Special characteristics of the data controller	The nature and role of the controller and its activities may affect the level of risk to individuals as a result of a breach. For example, a medical organisation will process special categories of personal data, meaning that there is a greater threat to individuals if their personal data is breached, compared with a mailing list of a newspaper.	
The number of affected individuals	Generally, the higher the number of individuals affected, the greater the impact of a breach can have. However, a breach can have a severe impact on even one individual, depending on the nature and context of the personal data that has been compromised. Again, the key is to consider the likelihood and severity of the impact on those affected.	

Conclusion

Based on my assessment against the factors above and on the facts available to me at this time, I consider that this breach is likely / not likely to result in a risk to the rights and freedoms of individuals, and that NEBDN is therefore required / not required to report the breach to the ICO, and that it is necessary / is not necessary to inform the individuals concerned.

NEBDN will review the circumstances of the breach and the outcome of the investigation and identify any ways that we can improve our policies and processes to minimise the likelihood and potential impact of future breaches.

Recommendations

1. The breach should be recorded in NEBDN's log. Reminders need to continue to be issued to staff about day to day examples of good and bad practice in data protection and information management
2. .
3. .

Completed by:	**Date:**

If the outcome of the risk assessment is that a breach is likely to result in a risk to the rights and freedoms of individuals, the following form should be used to notify ICO and (if necessary) the Charity Commission. If the outcome of this assessment indicates that a breach is likely to result in a high risk to the rights and freedoms of individuals, steps should be taken without delay to inform those individuals.

See also Appendix 6 which provides guidance on whether the Charity Commission should also be notified.

Notification of breach of personal data	
Organisation	**National Examining Board for Dental Nurses**
Nature of the personal data breach	
The categories and approximate number of individuals concerned	
The categories and approximate number of personal data records concerned	
A description of the likely consequences of the personal data breach	
A description of the measures taken, or proposed to be taken, to deal with the personal data breach	
The measures taken to mitigate any possible adverse effects (where appropriate)	
Name and role of lead person in the organisation	

Contact details of lead person in the organisation	
Signature and date	

Appendix 6: information to be considered as to whether to report a data breach to the Charity Commission and the other charity regulators in Scotland and Northern Ireland

Along with reporting a data breach to the ICO, a charity will also need to consider whether the data breach is a serious incident, and if so whether to report to the Charity Commission. The following data breaches should be reported to the Commission:

- Charity's data has been accessed by an unknown person - this data was accessed and deleted, including the charity's email account, donor names and addresses.
- A charity laptop, containing personal details of beneficiaries or staff, has been stolen or is missing.
- Charity funds lost due to an online or telephone 'phishing scam', where staff/trustees were conned into giving out bank account details.
- A data protection breach has occurred and been reported to the ICO.

Further information can be found about reporting a serious incident at:
https://www.gov.uk/guidance/ how-to-report-a-serious-incident-in-your-charity

Appendix 7: Confidentiality Undertaking

To be signed by every individual prior to undertaking any work for, or receiving information about, NEBDN. Different roles require that a confidentiality undertaking is completed at set points in time or at agreed time intervals. See chart that follows the undertaking for these time periods.

I acknowledge that I may, in the course of the work that the NEBDN has asked me to carry out, obtain information (whether or not in documentary form) relating to the NEBDN and its internal affairs, and information about individuals or third parties.

Bearing this in mind, I undertake:

a. to comply with the requirements of the General Data Protection Regulation 2016, Data Protection Act 2018, and the confidentiality requirements of the Financial Services and Markets Act 2000
b. not to disclose this information to any person without the NEBDN's prior written consent, unless this is strictly necessary to perform the work that the NEBDN has asked me to carry out
c. to take all reasonable steps to ensure that no other person gains access to information in my possession, and to inform the NEBDN immediately if I learn that a person not duly authorised has gained access to it
d. to immediately return documents I obtain in carrying out this work (and any copies made), on the NEBDN's request.

I accept that these obligations will continue to apply even when the work is completed.

In addition, I acknowledge that, where disclosure of the information I obtain is controlled by statutory provision, I may be prosecuted for wrongful disclosure.

Signed ……

Print name ……

Dated ……

Timing of completing a confidentiality undertaking in different roles

All roles require that an individual completes a confidentiality undertaking prior to them starting in a role with the NEBDN.

Role	Time at which confidentiality undertaking(s) must be completed
Staff	• Prior to taking up post • Annually – at point of appraisal?
Trustees	• Prior to taking up post • Annually
NEBDN Advisers	• Prior to taking up post • When reappointed (i.e. after three years)
Committee members	• Prior to taking up post • Annually
Examination super-coordinators	• Prior to every examination in which they are involved
Examiners	• Prior to every examination in which they are involved
Exam Helpers	• Prior to every examination in which they are involved
Exam Candidates	• ?
Witnesses (RoE/RoC)	• ?
Witness Markers	• ?