NCCA
An Chomhairle Náisiúnta Curaclaim agus Measúnachta
National Council for Curriculum and Assessment

NCCA Data Protection Policy

December 2023

Development and approval of policy

Policy developed by Data Protection Team	Q1 – Q2 2018
Approved by Council	Q2 2018 (June meeting)
Policy reviewed and updated by Data Protection Team	Q3 2019
Approved by Council	Q2, 2020 (September meeting)
Policy reviewed and updated by Data Protection Team	Q3 2023
Approved by Audit and Risk Committee	Q4 2023
Approved by Council	Q4 2023 (December meeting)

Contents

Introduction

The National Council for Curriculum and Assessment (NCCA) is a statutory agency under the aegis of the Department of Education (DE). NCCA advises the Minister for Education on curriculum and assessment for early childhood, primary and post-primary education. NCCA strives to fulfil the requirements of the Data Sharing and Governance Act (2019), Data Protection Bill 2018, the General Data Protection Regulation (GDPR) and the Law Enforcement Directive 2016/680 which set out the necessary standards in relation to protecting data subjects' privacy rights and to processing personal data.

NCCA is both a data controller and a data processor. This policy document sets out the responsibilities of the organisation in relation to data protection and outlines the basic principles by which it gathers and processes personal data in fulfilling these responsibilities. Key terms used in the policy are set out directly below.

Glossary of key terms

Consent	Permission voluntarily given for something to happen or agreement to a course of action. Consent can only be given by adults (over 18 years of age).
Assent	The expression of approval or agreement. Assent is sought from minors in conjunction with a relevant adult's consent for the same approval or agreement.
Data controller	The natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.
Data processor	A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.
Data processing	An operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the data.
Data Protection Impact Assessment (DPIA)	A Data Protection Impact Assessment (DPIA) describes a process designed to identify risks arising out of the processing of personal data and minimisation of these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance, including ongoing compliance, with the GDPR.
Data subject	A data subject is any person whose personal data is being collected, held or processed.
Personal data	Any information relating to an identified or identifiable natural person (data subject) 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.
Sensitive personal data	Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. That personal data includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying

Legal basis for gathering and processing personal data

The NCCA's role is set out in Article 41 of the Education Act (1998):

> *41.—(1) The object of the Council shall be to advise the Minister on matters relating to—*
>
> *(a) the curriculum for early childhood education, primary and post-primary schools, and*
>
> *(b) the assessment procedures employed in schools and examinations on subjects which are part of the curriculum.*

As such, collecting and processing personal data is part of NCCA's work in fulfilling its statutory remit in advising the Minister for Education on curriculum and assessment. In the case of working with the Department for Children, Equality, Disability, Integration and Youth, early childhood settings, schools and children in care and detention centres, the Council seeks consent/assent from the individuals involved in the work. This includes consent from educators/teachers, managers/principals and parents/guardians as well as consent from young people under 18 years of age.

NCCA also works with experts in education, networks of professionals, researchers and companies where personal, financial and other data is required to be collected and stored to issue payments and contracts, where applicable.

Data subjects and types of personal data

In fulfilling its statutory remit, NCCA collects and processes personal data from individuals such as:

- employees
- contractors
- commissioned staff
- members of Development Groups, Boards and Council
- individuals who have engaged with an NCCA consultation
- individuals who participate in setting/school-based work

- individuals and registered teachers who open accounts on curriculumonline.ie
- experts in education, networks of professionals, researchers and companies where personal, financial and other data is required to issue payments and contracts.

The categories of personal data held by NCCA include, amongst others, contact details, financial details, garda vetting, and human resources data. In the case of individuals in educational settings working with NCCA, or presenting at NCCA conferences, the personal data may also include:

- video recordings
- audio recordings
- photographs
- reproduction of hand-drawn and written work.

The multi-media content is stored by NCCA, edited for publications and may be used to support the work of NCCA, presented at NCCA events, and published on the organisation's websites. All categories of personal data have been identified in NCCA's Record of Processing Activities (RoPA).

Seven key principles

NCCA's approach to, and work in processing personal data is underpinned by the following seven principles which are core to the GDPR. Each principle is described briefly below. The Council uses a suite of documentation to inform data subjects about what personal data is gathered and how and why it is processed. This documentation includes the Data Protection Policy, privacy notices, data sharing agreements, contracts/Service Level Agreements (SLAs) and forms such as consent and assent forms, job application forms, commissionee forms and travel and subsistence forms.

1. **Lawfulness, fairness and transparency**

   Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

   This principle relates to the data controller/processor having a lawful basis for gathering and processing personal data and for informing data subjects when personal data is being gathered, what data is being gathered and for what purpose(s). NCCA gathers only personal data needed to carry out its statutory remit under Article 41 in the Education Act (1998) and informs data subjects, at the point of collection, how the data will be processed used.

2. **Purpose limitation**

   Personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

   The principle relates to data being used solely for the purpose(s) communicated to data subjects. NCCA informs data subjects of the purpose(s) for which their personal data is collected, and uses the data for the intended purpose(s) only.

3. **Data minimisation**

Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

This principle relates to restricting data collection to the data needed for a specified purpose and avoiding unnecessary duplication of that data. NCCA collects and holds only data needed for the Council to carry out its statutory remit as under Article 41 in the Education Act (1998).

4. **Accuracy**

Personal data must be accurate and, where necessary, kept up to date.

This principle relates to the importance of ensuring, as far as is practicable, that personal data stored is accurate. NCCA takes every reasonable step to ensure that the personal data which it holds is accurate. Data subjects have a responsibility to ensure that at the point of collection, the data is correct. Data subjects can contact NCCA at any time and request that personal data is updated and/or corrected.

5. **Storage period limitation**

Personal data must be kept for no longer than is necessary for the purposes for which the personal data are processed.

This principle relates to holding personal data for no longer than is necessary. Taking account of relevant retention periods in fulfilling legal and contractual requirements, NCCA deletes data once the purpose(s) for which it was intended is fulfilled. Exceptions to this may include situations where the data is needed as part of a disciplinary process, appeals process, legal case or is further anonymised and aggregated for the purposes of making it available as open data under the Open Data and re-use of Public Sector information Directive) (EU) 2019/1024, which was transposed into Irish law by SI 376/2021 on July 22nd 2021.

6. **Integrity and confidentiality**

Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical and organisational measures.

This principle relates to the importance of personal data being stored safely and securely with access only by authorised persons. NCCA uses secure IT-platforms and software for storing personal data and takes reasonable and practical measures to prevent personal data from being stolen, misused, or abused, and to prevent personal data breaches. Staff with access to personal data are either directly involved in using the data and/or have oversight of the work. Access to the IT-platforms and software is password protected. In addition, NCCA computers and tablets, in line with measures being taken in the wider area of cybersecurity, are encrypted, require multi-factor authentication for access. and have backend authentication. Each device can be disabled remotely and wiped, deleting all data

including personal data in the event of the device being stolen or mislaid. Where a device has been recovered all data can be restored to its user. Further information on the security of data is set out in NCCA's Acceptable Use, Emails and Access, Mobile Phone and IT policies.

7. **Accountability**

   The controller is responsible for, and must be able to demonstrate, their compliance with all of the above-named Principles of Data Protection; take responsibility for the processing of personal data and GDPR compliance; and be able to demonstrate (through appropriate records and measures) this compliance, in particular to the Data Protection Commissioner.

   This principle relates to the ability to demonstrate adherence to the principles of data protection as outlined above and having clear lines of responsibility for the data. NCCA takes every reasonable step to ensure compliance with data protection requirements. See Responsibilities section below for further information.

Embedding a risk-based approach to data protection

NCCA uses a risk-based approach to data processing. NCCA has established a risk register dedicated to cyber and data risks, which identifies risks associated to processes and activities across the organisation and describes actions to mitigate them. This register is kept under review by the Chief Information Officer and senior management team, the Data Protection Team and the Audit and Risk Committee. Adopting this risk-based approach helps to embed the principles of data protection in the work of the organisation.

Data subjects' privacy rights

As a data controller and data processor, NCCA acts to ensure the upholding and protection of data subjects' privacy rights. These include the right to:

- be informed about the collection and use of their personal data by NCCA
- access the personal data held on an individual, and to request this data in a portable format
- have the personal data corrected and/or updated if any part of that data is inaccurate or incomplete
- be forgotten—to ask NCCA to delete the personal data held on an individual. This must, however, be done in compliance with any legal or statutory obligations.
- restrict or cease the processing of an individual's personal data
- object to NCCA using an individual's data for a particular purpose(s). nh

Data portability

Data subjects have the right to receive, upon request, a copy of the data which they provided to NCCA. They have a right to receive this in a structured format enabling them to transfer the data to

another controller/processor. As per the GDPR, NCCA does not charge for this service. Requests to receive a copy of data in a portable format are processed as Data Subject Access Requests. These requests will be processed within 30 days provided they are not excessive and do not impinge on the rights of other individuals. For information on this process, see the Data Subject Access Request Policy in Appendix A and the Data Subject Access Request Form in Appendix B.

Disclosure to third parties

Where NCCA uses third parties to collect and/or process personal data on its behalf, a Data Sharing/Processing Agreement will be put in place. Examples of work involving such Agreements include the use of third parties to gather, analyse and/or report data as part of consultations or research projects, data shared for auditing purposes and the sharing of multi-media materials with support services. The Data Sharing/Processing Agreement sets out the purpose of the sharing/processing, the categories of data concerned, and the need for the third party to ensure that appropriate measures are in place to safeguard the personal data. The third party is not permitted to use the data for any purpose other than that specified by NCCA in the Data Sharing/Processing Agreement. The level of detail included in the agreement is influenced by the categories of personal data being shared, the quantity of data involved, and the risks associated with the transfer.

The Data Sharing and Governance Act (2019) was established to provide the legal basis for public bodies to share data. NCCA, when sharing data with other Government departments or bodies, will use this mechanism, through the Data Governance Board, as part of the Government's drive to provide transparency on the efficient use of citizen data to deliver public services.

Data Protection Impact Assessments

In light of the risk-based approach to data protection which NCCA adopts, and the importance of taking account of privacy considerations from the beginning when planning areas of work, NCCA will complete Data Protection Impact Assessments (DPIAs) where this is deemed helpful or necessary. The DPIA is a process of systematically considering the potential impact that a project or initiative might have on the privacy of individuals. The DPIA will enable NCCA to identify potential privacy issues before they arise and come up with a way to mitigate them. If and where the DPIA shows that the risks identified cannot be fully mitigated, NCCA will consult the Data Protection Commissioner.

In the case of tenders for research and where the gathering of personal data on a large scale is involved, NCCA requests that tenders provide information on data protection including processes, safeguards, risk analysis, and mitigating factors. The research contracts, in turn, set out the data controller/processor arrangements.

Communicating with data subjects

Before, or at the time of collecting personal data as part of NCCA's work, data subjects will be informed of the following:

- the types of personal data collected
- the purpose(s) for using the data

- processing methods
- the data subjects' rights with respect to their personal data,
- the retention period,
- if data will be shared with third parties.

In the case of NCCA's work with early childhood settings and schools, and where consent and assent are sought to gather multi-media recordings and/or examples of young peoples' work, the information above is provided in a letter to each parent/guardian and student where they are 18 years of age. Assent is also sought from those young people who are under 18 years of age. In the case of users visiting NCCA websites, the information is provided through the website privacy statement.

Consent

As outlined previously, NCCA collects and processes personal data to fulfil its statutory remit under Article 41 of the Education Act (1998) and seeks consent from all individuals to gather and process their data for specified purposes. NCCA obtains specific, informed and freely given consent from all individuals from whom data is collected. This is ensured through documenting the affirmative consent. Individuals may withdraw their consent at any time and individuals are informed of this right prior to giving consent.

A key aspect of NCCA's work is engagement with young people. To support this work NCCA seeks consent from each young person aged 18 and over and from the parents/guardians of those under 18, and where relevant, staff. In the case of young children under 18 their assent is sought once their parents have given consent. Modified assent forms are being developed for younger children and for those with additional needs. Young people are not identified by name in any recordings or on any written work.

Feedback from settings/schools and from staff across the organisation is used to inform periodic reviewing and updating of the consent forms as necessary. NCCA acknowledges the importance of informed consent/assent and endeavour to provide these forms using plain English for adults and young people alike.

Data breaches

NCCA takes all reasonable steps to ensure that personal data is stored securely and confidentially. However, data breaches can and do happen. NCCA has a formal process for responding to breaches and near-breaches if, and when, they occur. This includes clearly defined procedures for internal reporting of breaches, investigation of the breaches, appropriate decision-making in responding to the breaches, and where necessary, reporting the breaches to the relevant data subjects, and to the Data Protection Commissioner within the statutory 72 hours. See Appendices C and D for the Data Breach Policy and the Pro forma.

A log is retained of breaches and near-breaches and this informs the ongoing work of the Data Protection Team in reviewing and responding to risks. On a regular basis, NCCA runs threat management simulations to assess the integrity of our cloud resources. The simulations include:

- spear phishing/credential harvesting attacks to attempt to acquire sensitive information such as usernames, passwords and other personal information
- brute force attacks which is a trial-and-error method of generating multiple password permutations to break user accounts in the azure directory
- password spray attacks using commonly used passwords to break user accounts in the azure directory.

As with the log, learning gained from these simulations feed into the work of the Data Protection and IT Teams.

Responsibilities

All staff in NCCA are responsible for ensuring that they process personal data in an appropriate manner which meets the standards set out in this policy. To enable this, all staff have been provided with CPD on data protection with this being augmented over time with CPD on specific aspects of data protection such as cybersecurity. It is also factored into the induction training of all new staff.

As a public body, NCCA has a Data Protection Officer (DPO) with overall responsibility for data protection. In addition, the organisation has a Deputy DPO (DDPO) who is also a member of the IT Team providing a direct link between data protection and IT which is particularly important in the area of cybersecurity. The DPO and DDPO are supported in their work by a Data Protection team which draws its members from across the organisation and reports directly to the CEO. The DPO also provides updates to the relevant members of staff on work related to data protection. Members of the Data Protection Team have completed accredited training in the area.

Appendix A: Data Subject Access Request Policy

Introduction

Under GDPR, all individuals have a right to request access to their personal information. A Data Subject Access Request (DSAR) outlines how outlines how the National Council of Curriculum and Assessment (NCCA) responds to and handles requests made by individuals for access to their personal data. The purpose of the policy is to enable NCCA to:

- comply with our obligations under GDPR, and in particular, to respond in a timely and appropriate manner to a DSAR;
- ensure that information held about data subjects is accurate and up to date; and
- increase the level of trust by being open with individuals about the information that is held about them.

Who is this DSAR procedure for?

The procedure is for individuals for whom NCCA holds data. This list for example, while not exhaustive, includes:

- video recordings
- audio recordings
- photographs
- reproduction of hand-drawn and written work
- current and past employees either permanent or temporary
- current and past contractors
- current and past commissioned staff
- current and past members of subject Development Groups, Boards or Council
- individuals who have engaged with an NCCA consultation
- individuals, past and present who have participated in an NCCA network.

Rights of a data subject

If personal information is being processed, a data subject has the following rights:

- to know whether a data controller holds any personal data about them.
- to receive a description of the data held about them and, if permissible and practical, a copy of the data.
- to be informed of the reason(s) for which their data is being processed, and from where it was received.
- to be informed whether the information is being disclosed to anyone apart from the original recipient of the data; and if so, the identity of those recipients.
- the right to data portability. Data subjects can ask that their personal data be transferred to them or a third party in machine readable format (JPG, MP4 movie, Word, PDF, etc.).

However, such requests can only be fulfilled if the data in question is: 1) provided by the data subject to NCCA, 2) is processed automatically and 3) is processed based on consent or fulfilment of a contract.

- the right to rectify incorrect personal data that is held.
- the right to erase personal data. This is only applicable in certain circumstances and is not an absolute right. The data subject can request erasure of their personal data if:
    - the personal data is no longer necessary for the purpose which NCCA originally collected or processed it for
    - NCCA are relying on consent as the lawful basis for holding the data, and the individual withdraws their consent.

Data Subject Access Requests (DSARs) in writing

A Data Subject Access Request (DSAR) is any request made by an individual or parent/guardian on behalf of their child for information held about them by NCCA. A DSAR must be made in writing, either electronically or by post. Verbal requests for information held about an individual will not be processed by NCCA. A DSAR Form will be provided to an individual who wishes to make a request (see Appendix B). However, if assistance is required by the applicant, NCCA will endeavour to provide help.

In the event that a DSAR is made verbally to a staff member of NCCA, further guidance should be sought from **NCCA's Data Protection Officer** who will direct the individual to the DSAR Form and inform the individual that the request should be made in writing. NCCA will not provide personal information via social media channels.

DSAR process

Step 1: Request for information

To enable NCCA to respond to DSARs in a timely manner, the individual data subject or parent/guardian of a child should:

- Submit their request using NCCA's Data Subject Access Request Form.
- Provide the NCCA with sufficient information to validate their identity (to ensure that the person requesting the information is the data subject or an individual authorised by the data subject).

Subject to the exemptions referred to in this policy, NCCA will provide information to data subjects where requests are made in writing and are received from an individual whose identity can be validated by NCCA.

However, NCCA may not provide data where the resources required to identify and retrieve the requested data would be excessively difficult or time-consuming. For example, if the data subject is asking for all data that the organisation has ever collected about this person, this might require too much time and resources to fulfil the request. In this case, NCCA will invite the data subject to

request more specific information. Requests are more likely to be successful where they are specific and targeted at particular information. Factors that can assist in narrowing the scope of a search include use of the Project Identifier, identifying the time period in which the information was gathered and being specific about the nature of the data sought (for example, a copy of a particular form, video footage, photographs, email records).

Step 2: Identity Verification

NCCA's Data Protection Officer will check the identity of anyone making a DSAR to ensure information is only given to the relevant person. The DSAR Form requires the data subject to provide two forms of identification, one of which must be a photo identity and the other confirmation of address. If the requestor is not the data subject, written confirmation that the requestor is authorised to act on behalf of the data subject is required.

Note: While the right of access by the data subject under Article 15 of GDPR applies to a person's own personal data, it would also be reasonable to comply with an access request submitted on a person's behalf in the case of a child, by a parent or guardian. In this case, the Data Protection Officer should be satisfied that the requestor is acting on behalf of, and in the best interests of the child whose data is being requested.

Step 3: Information for the Data Subject Access Request

Where the NCCA's Data Protection Officer is reasonably satisfied with the information presented by the requestor (i.e. a completed DSAR form and identification verification if necessary) the Data Protection Officer will notify the requestor that their DSAR will be responded to within 30 calendar days. The 30-day period begins from the date that all necessary documents are received from the requestor.

Step 4: Review of Information

NCCA's Data Protection Officer will gather all the information as requested in the DSAR and will ensure that the information is reviewed, as far as is practicable, to ensure completion with the 30-calendar day timeframe.

Step 5: Response to the Access Request

NCCA's Data Protection Officer will ensure that a written response is sent back to the requestor. This will be via email, unless the requestor has specified another method by which they wish to receive the response (for example, post). NCCA will only provide information via channels that are secure. When hard copies of information are posted, they will be sealed securely and sent by recorded delivery. When documents are emailed, they will be password protected (encrypted) and the password sent to the requestor by separate means.

Step 6: Archiving

After the response has been sent to the requestor, the DSAR will be considered closed and archived by NCCA's Data Protection Officer.

Exemptions

An individual does not have the right to access information recorded about someone else, unless they are an authorised representative, or have parental responsibility or guardianship. NCCA is not required to respond to requests for information unless provided with sufficient details to enable the location of the information to be identified and can be satisfied as to the identity of the data subject making the request.

In principle, NCCA will not normally disclose the following types of information in response to a Data Subject Access Request:

- Information about other people:
  A DSAR may cover information which relates to an individual or individuals other than the data subject. Access to such data will not be granted, unless the individuals involved consent to the disclosure of their data. Information relating to other individuals will be redacted, if and where necessary, to ensure anonymity.
- Repeat requests:
  Where a similar or identical request in relation to the same data subject has previously been submitted and responded to within a reasonable time period, and where there is no significant change to the personal data held in relation to that data subject, any further request made within a 3-month period of the original request will be considered a repeat request, and NCCA will not provide a further copy of the same data.
- Publicly available information:
  NCCA is not required to provide copies of documents which are already in the public domain.
- Opinions given in confidence or protected by copyright law:
  NCCA does not have to disclose personal data held in relation to a data subject that is in the form of an opinion given in confidence or protected by copyright law.

DSAR refusals

There are situations where individuals do not have a right to see information relating to them. For instance:

- If the information is kept only for the purpose of statistics or research, and where the results of the statistical work or research are not made available in a form that identifies any of the individuals involved.
- Requests made for other, non-data protection purposes can be rejected.

If the Data Protection Officer refuses a DSAR on behalf of NCCA the reasons for the rejection will be clearly set out in writing. Any individual dissatisfied with the outcome of their DSAR is entitled to make a request for the outcome to be reviewed.

Appendix B: Data Subject Access Request (DSAR) Form

NCCA An Chomhairle Náisiúnta Curaclaim agus Measúnachta National Council for Curriculum and Assessment

National Council for Curriculum and Assessment
Data Subject Access Request Form

You have the right to request personal data we may hold about you. This is known as a Data Subject Access Request (DSAR). If you wish to make a DSAR, please complete this form and return to us by post or email.

1. Details of the person requesting the information

Full Name:	Date of Birth:		
	DD	MM	YYYY

Contact Address:

Contact Details:	
Home Number:	Mobile Number:
Email:	

2. Are you the data subject?

Yes: If the information is about you, please supply a copy of a of government issued photographic identification, for example, Passport or Driver's Licence and a proof of address such as a utility bill.

No: If you are acting on behalf of the data subject with their written authority; this authority must be sent to us and complete section 4.

Government ID:		Tick that document is included	Proof of Address:		Tick that document is included

3. Details of data requested

Please describe the information you seek together with any other relevant information. This will help us identify the information you require.

3.1 Data Subject Access Request for Video or Photographic imagery

If you are making a Data Subject Access Request for video or photographic imagery that we retain, we will use the image in your Government Photographic Identification to assist us.

3.2 Parent's/Guardian's request for video or photographic imagery on behalf of their child

If you are making a Data Subject Access Request for video or photographic imagery as a Parent/Guardian on behalf of your child, you will be required to provide us with a photograph to identify the data subject/child. If you are sending a request by post, please print a clear and identifiable image and include it in your request. If you are emailing your request, please attach the image to your email application. Do not send original photographs; please send us copies. NCCA will delete any imagery after the Data Subject Access Request is completed.

Photograph is included:		Tick that photograph is included

4. Who will the NCCA send the DSAR information to?

The DSAR applicant has the option to decide to whom the requested material should be sent.

Send the requested information to:

Data Subject:		Tick to indicate	Data Subject's Representative		Tick to indicate

Permission for the information to be released to an authorised representative.

I give my permission for _____ (fill out the name of the authorised representative) to have access to my personal data.

Signature of Data Subject:	Print Name:
Date:	

Confirmation of the authorised representative of the Data Subject.
To be filled out by the representative of the Data Subject
I confirm that I am the authorised representative of the Data Subject.

Name:	Address:
Signature:	Date:

Please send me the Data Subject's information by:

Registered Post:		Tick to indicate	Email:		Tick to indicate

Post Request	Email
If sending by post, please use the following address: **Data Protection Officer** **National Council for Curriculum and Assessment,** **ESRI Building,** **Whitaker Square,** **Sir John Rogerson's Quay,** **Dublin 2,** **D02 K138,** **Ireland**	If sending by email, please use the following address: **dpo@ncca.ie** Please write "Data Subject Access Request" in the subject field of the email.

National Council of Curriculum and Assessment - Data Subject Access Requests

We will make every effort to process your data subject access request as quickly as possible within 30 calendar days. If you have any queries while your request is being processed, please do not hesitate to contact us at this email address: dpo@ncca.ie

Appendix C: NCCA Data Breach Policy

Introduction

The National Council for Curriculum and Assessment (NCCA) is a statutory agency under the aegis of the Department of Education (DE). The NCCA advises the Minister for Education on curriculum and assessment for early childhood education, primary and post-primary schools. NCCA strives to fulfil the requirements of the Data Protection Bill 2018, the General Data Protection Regulation (GDPR) and the Law Enforcement Directive 2016/680 which set out higher standards in relation to protecting data subjects' privacy rights and to processing personal data.

From 25th May 2018, the GDPR introduced a requirement for organisations to report personal data breaches to the relevant supervisory authority, where the breach presents a risk to the affected individuals. Organisations must do this within 72 hours of becoming aware of the breach. Where a breach is likely to result in a high risk to the affected individuals, organisations must also inform those individuals without undue delay.

NCCA adopts a risk-based approach to data protection and actively seeks to identify risks associated with its processing of personal data in order to take appropriate actions to mitigate these risks. Data breaches, however, can still occur regardless of technical or physical measures. Human error can also lead to a breach. This policy document outlines the responsibilities of NCCA in the case of data breaches including the obligation to notify the Data Protection Commissioner and other relevant individuals as required under GDPR. The policy also sets out the process through which the organisation responds to breaches (and near-breaches) and mitigates against future breaches within the organisation.

Data breach response procedure

All data breaches within and by NCCA should be reported to the organisation's Data Protection Officer (DPO) at dpo@ncca.ie or 087 635 3658 as soon as possible. Once a personal data breach is reported to or detected by the DPO, the following Data Breach Response Procedure is initiated.

Step 1	Identify and confirm that a breach has occurred. The DPO in collaboration, where possible, with the Data Protection Team is responsible for determining if the breach should be considered a breach affecting personal data.
Step 2	Take immediate action to stop the breach if it is ongoing or to reduce the affected data.
Step 3	Ensure proper and impartial investigation is initiated, conducted, documented, and concluded. The Data Breach Register will be used to record this information. The DPO is responsible for documenting all decisions and actions in relation to the breach. This may be reviewed by the Irish Data Protection Commissioner's Office and therefore will be written as precisely and thoroughly as possible to ensure traceability and accountability.
Step 4	Identify remediation requirements and document the remediation.
Step 5	Notify the Irish Data Protection Commissioner's office if required. Not all personal data breaches need to be notified to the Office. The notification obligations under the

	GDPR are only triggered when there is a breach of personal data which is likely to result in a risk to the rights and freedoms of individuals. The DPO, in collaboration, where possible, with the Data Protection Team, will establish whether the personal data breach should be reported to the Irish Data Protection Commissioner's Office.
Step 6	Coordinate internal and external communications. The DPO will assess the risk associated with the personal data breach and determine if the breach needs to be reported.

Breach notification process

To facilitate decision-making and determine whether or not the organisation needs to notify the DPC and affected individuals, NCCA uses a quality risk management process and breach detection, investigation and reporting processes. In determining how serious the breach is for affected individuals, account is taken of the impact the breach could potentially have on individuals whose data has been exposed. In assessing this potential impact, the following are considered:

- the nature, sensitivity and volume of the personal data in question
- the cause of the breach
- the type of data exposed
- the ease of identification of individuals from the data
- the severity of consequences for individuals
- special characteristics of the individual(s) – e.g. a breach affecting vulnerable individuals may place them at a greater risk of harm
- the number of affected individuals
- mitigating factors in place and whether the personal data of vulnerable individuals has been exposed.

As provided by the DPC Office, the NCCA uses the following guide to define levels of risk.

Low risk	The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal.
Medium risk	The breach may have an impact on individuals, but the impact is unlikely to be substantial.
High risk	The breach may have a considerable impact on affected individuals.
Severe risk	The breach may have a critical, extensive or dangerous impact on affected individuals.

Initial notification of a breach

If a breach is likely to result in a risk to the rights and freedoms of the affected data subjects, the DPO will notify the affected data subjects without delay. The notification to the data subjects will be written in clear and plain language using the Data Breach Notification Form – Data Subject. If, due to the number of affected data subjects, it is disproportionately difficult to notify each affected data subject, the DPO will take the necessary measures to ensure that the affected data subjects are notified using appropriate, publicly available channels.

Where a report is to be made to the DPC Office, this is done using the National Breach Notification Form (Appendix A – form provided by the DPC Office) and emailed to breaches@dataprotection.ie. The subject line in the email indicates:

- whether the breach is 'new' or an 'update' to a previous breach notification
- the NCCA's name
- the self-declared risk rating for the breach.

An example of an email subject line is New Breach Report, NCCA, High Risk

The report is made as soon as possible and within 72 hours of the DPO being made aware of the breach. If the report is made beyond 72 hours, the reason for this is communicated to the DPC Office.

If the personal data breach is not likely to result in a risk to the rights and freedoms of the affected data subjects, no notification is required. In these instances, the data breaches are recorded in the NCCA's Data Breach Register which includes details of basis for the decision that there was no risk, who made this decision, and the risk rating assigned to the breach.

If a data processor (i.e. third party) is responsible for a breach

NCCA as the data controller, will ensure that an agreement is in place between all third-party processors (e.g., payroll provider, accountants, video editors) to ensure personal data is protected. If a personal data breach or suspected breach occurs within the third party, the third party will report this to the NCCA's DPO without undue delay. In doing this, the third party includes the following:

- a description of the nature of the breach
- categories of personal data affected
- approximate number of data subjects affected
- name and contact details of the DPO
- consequences of the personal data breach
- measures taken to address the personal data breach
- any other information relating to the data breach.

The breach response procedure and breach notification process are then followed as necessary.

Appendix D: Pro forma for reporting a Data Breach

Pro forma for reporting a Data Breach

If you discover a personal data security breach or near-breach, please notify the NCCA's Data Protection Officer immediately at 01 661 7177 and dpo@ncca.ie. Please complete this form to provide details of the breach and send it to dpo@ncca.ie.
In the form below, all references to a breach include near-breaches.

Date(s) of the Personal Data Breach	
Time of the Personal Data Breach	
Date and time the breach was discovered	
Name of person who discovered the breach	
Contact details of the person who discovered the breach	
Brief description of the breach	
Number of data subjects affected, if known	
Estimated level of risk to data subjects' privacy** (see table below)	
Brief description of actions, if any taken, since breach was discovered	

Name of person reporting the breach _____ Print name	Name of person receiving the report _____ Print name
Signature of person reporting the breach _____ Signature	Signature of person receiving the report _____ Signature
_____ Date	_____ Date
Contact details of person reporting the breach:	Action taken:
	_____ Date taken

**Categorisation of risk associated with data breaches

Low risk	The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal.
Medium risk	The breach may have an impact on individuals, but the impact is unlikely to be substantial.
High risk	The breach may have a considerable impact on affected individuals.
Severe risk	The breach may have a critical, extensive or dangerous impact on affected individuals.

NCCA

An Chomhairle Náisiúnta
Curaclaim agus Measúnachta
National Council for
Curriculum and Assessment