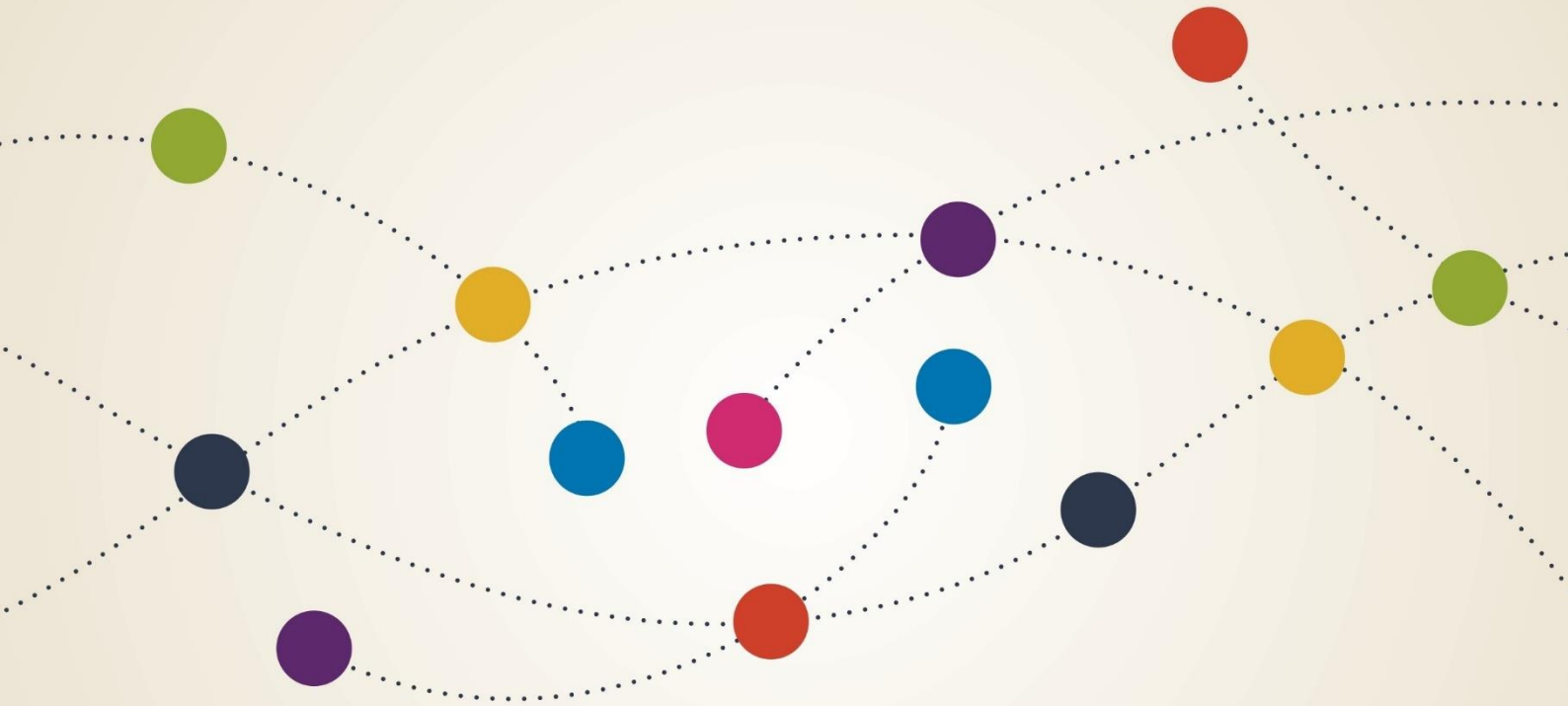


NCCA Data Protection Policy

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

September 2020

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	Q3 2019 (September meeting)
Policy reviewed and updated by Data Protection Team	Q3 2020
Approved by Council	Q3 2020 (September meeting)

Contents

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 on curriculum and assessment for early childhood education, primary and post-primary schools. The NCCA strives to fulfil the requirements of the Data Sharing and Governance Act (2019)[1], Data Protection Bill 2018, the General Data Protection Regulation 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.

The NCCA is 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 in a Glossary of Terms in Appendix A.

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, processing personal data is part of the NCCA's work in fulfilling its statutory remit in advising the Minister for Education on curriculum and assessment matters from early childhood through to senior cycle education. In the case of working with early childhood settings and schools, the Council also seeks consent from the individuals involved in the work.

[1] The Data Sharing and Governance Act (2019) was signed into Irish law on March 4th, 2019 and is awaiting commencement. The Act is intended to provide for more efficient and cost- effective service delivery by public bodies by providing a clear legal basis for sharing personal data in certain circumstances. The Act sets out specific requirements for data sharing agreements including the need to review them every five years. The Act excludes Special Category Data.

These include children/students, parents/guardians, practitioners/teachers, and managers/principals.

Data subjects and types of personal data

In fulfilling its statutory remit, the NCCA gathers and processes personal data from the following individuals:

- employees
- contractors
- commissioned staff
- Council members, members of boards and development groups
- individuals who have engaged with an NCCA consultation
- individuals who participate in setting/school-based work
- individuals involved in research.

The categories of personal data held by the NCCA include contact details, financial details, garda vetting, and human relations data. In the case of individuals in educational settings working with the NCCA, the personal data may also include:

- video recordings
- audio recordings
- photographs
- reproduction of hand-drawn and written work
- Teaching Council registration numbers.

The multi-media content is stored by the NCCA, edited for publications used to support the work of the NCCA, presented at NCCA events, and published on the organisation's websites.

Seven key principles

The NCCA's approach to, and work in processing personal data is underpinned by the following seven principles which are at the heart of the General Data Protection Regulation. 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 and forms such as consent 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). The NCCA gathers only personal data needed to carry out its statutory remit under Article 41 in the Education Act and informs data subjects, at the point of collection, how the data will be 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. The NCCA informs data subjects of the purpose(s) for which their personal data is gathered 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. The NCCA collects and holds only data needed for the Council to carry out its statutory remit as set out 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. The 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 the 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, the 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, or legal case.

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. The NCCA uses secure IT-platforms 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 is password protected. In addition, NCCA computers and tablets, in line with measures being taken in the wider area of cybersecurity, are encrypted 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 the NCCA's IT policy.

In the case of examples of student work, some of these are stored in a password-protected space on www.curriculumonline.ie. Access to this area is restricted to the NCCA staff working on the examples and teachers with active Teaching Council registration numbers.

The Coronavirus pandemic has necessitated the organisation moving to remote working since mid-March 2020. With the possibility of this continuing for some time, either fully or partially, the NCCA has continued to give particular attention to data protection in this environment and has prioritised the following measures:

- offering training to staff on using conferencing software with a focus on security practices
- ensuring every staff member has access to an NCCA-enrolled device for their work
- developing protocols for arranging external remote meetings
- adding extra security alerts that identify user accounts at risk from phishing attacks
- developing clear guidance on important, practical steps in protecting personal data (see Appendix B as an example).

To monitor these measures and to assess the need for further organisational supports, remote working is a standing agenda item at each IT Group and Data Protection Team meeting. Remote working has also been added to the Risk Register, acknowledging the associated risks, which include data protection, and identifying controls to help mitigate against these.

7. Accountability

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. The NCCA takes every reasonable step to ensure compliance with data protection requirements. See *Responsibilities* on page 13 for further information.

Embedding a risk-based approach to data protection

The NCCA uses a risk-based approach to data processing. In doing this, project teams include a focus on risk management as they plan, monitor and review work. This risk management approach includes data protection. Broader and more over-arching risks are identified by the Data Protection Team with mitigating actions taken and the risks kept under review. All of this feeds into and informs the organisation's main Risk Register. In turn, the main Risk Register is periodically reviewed by the Directors Group, by the Senior Management Team, the Audit and Risk Committee and by Council. Adopting this risk-based approach helps to embed the principles of data protection in the work of the organisation while also ensuring that the Risk Register takes account of new and emerging risks and associated mitigating actions.

Data subjects' privacy rights

As a Data Controller and Data Processor, the 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 the 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 the 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 the NCCA using an individual's data for a particular purpose(s).

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, the 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 C and the *Data Subject Access Request Form* in Appendix D.

Disclosure to third parties

The NCCA uses Data Sharing Agreements and Data Processing Contracts where third parties are involved in processing personal data on its behalf. Examples of work involving such arrangements include the use of third parties to gather, analyse and/or report data as part of consultations or research projects, and the sharing of multi-media materials with support services. Data Processing Contracts are also used for aspects of corporate governance

including financial services purchased by Council. The agreements and contracts set out the purpose of the processing, the data subjects, 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 the NCCA. See Appendix E for a sample. The level of detail included is influenced by the categories of personal data being shared, the quantity of data involved, and the risks associated with the sharing and processing.

Data Protection Impact Assessments

In light of the risk-based approach to data protection which the NCCA adopts, and the importance of taking account of privacy considerations from the beginning when planning areas of work, the NCCA will complete Data Protection Impact Assessments (DPIA) 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 the organisation 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, the 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, the 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 the 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 the NCCA's work with early childhood settings and schools, and where consent is sought to gather data in written format, through multi-media recordings and/or examples of children's/students' work, the information above is provided in a letter to each parent/guardian and student where they are 18 years of age. In the case of users visiting the NCCA websites, the information is provided through a privacy statement and a cookies statement. See Appendices F, G and H.

Consent

As outlined previously, the NCCA gathers and processes personal data in order to fulfill its statutory remit set out in Article 41 of the Education Act (1998). Exemplification of children's/student's work, and teaching and learning lie at the heart of the NCCA's development of curriculum specifications. This involves working directly with practitioners/teachers, managers/principals, children/students, and parents to gather video, audio, and photographic examples from early childhood settings and primary and post-primary schools. In doing this work, the NCCA seeks consent from each child/student and his/her parent/guardian, and staff. In the case of young children, assent is sought. In seeking consent, data subjects are informed of the purpose(s) of gathering examples and are made aware of how the examples will be used. In publishing examples of children's/students' work, surnames are not used in any recordings or on any written work. Data subjects can request

that their image is removed from the NCCA websites at any point in the future by contacting the NCCA's Data Protection Officer (DPO). See Appendices G and H for examples of NCCA consent documentation used in past projects. Drawing on feedback from schools and from staff across the organisation, the consent forms are reviewed periodically and updated as necessary.

At times, the NCCA commissions work involving third parties working with children, young people, practitioners, parents and school leaders. This is relevant in areas of research in particular. In these instances, the research contracts with the third parties set out the relevant data protection requirements, responsibilities and safeguards. Consent forms a key part of this.

Data breaches

As described above, the NCCA takes all reasonable steps to ensure that personal data is stored securely and confidentially. Data breaches, however, can happen. The NCCA has a 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, and informing the Audit and Risk Committee and Council. See Appendices I and J for the Data Breach Policy and the Data Breach Register proforma. A log is retained of near-breaches and breaches and this informs the ongoing work of the Data Protection Team in reviewing risks, identifying further mitigating strategies and taking appropriate actions in a timely manner.

As part of the cyber security practices within the NCCA, threat management simulations are regularly run to assess the integrity of the NCCA accounts. 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.

In addition to these simulations, the NCCA outsource further IT support which includes cybersecurity supports in the event of any attacks. The company responsible for this support are holders of ISO 27001 certification, the international standard for information security management.

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

Responsibilities

All staff in the NCCA are responsible for ensuring that their processing of personal data is appropriate and 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. Data protection forms part of the induction programme for staff on joining the organisation.

As a public body, the organisation has a Data Protection Officer (DPO) with overall responsibility for data protection. In addition, the organisation has a Deputy DPO who is also a member of the IT Team. In addition, the Chief Risk Officer who also oversees IT security is a member of the team providing a direct link between data protection and cybersecurity. The DPO and DDPO are supported in the work by a Data Protection team which draws its members from across the organisation and reports directly to the CEO (see page 2). Updates are provided to the Audit and Risk Committee on work related to data protection.

Members of the Data Protection Team have completed accredited training in the area.

Appendix A: Glossary of key terms

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 a natural person, data concerning health or sexual orientation.

Appendix B: Data Protection and working from home

The questions below relate to data protection in a remote working environment. The NCCA's Data Protection Policy continues to be relevant and applicable in a remote working context as it is in the office environment. The material below responds to and clarifies specific questions that have arisen from the need to move fully to remote working in response to the COVID-19 pandemic. This material is intended as a support for staff.

Can I use my personal device to start working on a document?

No. All NCCA documents and materials should be worked on using NCCA devices only. If you create or edit a document, please ensure it is on an NCCA-enrolled device. All NCCA devices have a profile that allows you to comment on documents when collaborating. On NCCA devices your name will appear whereas on personal devices all comments will appear as 'author' regardless of who is making the comments.

Creating and editing a document on an NCCA device ensures that your profile and the profiles of others in the organisation will be shown in the document.

Can other people at home use my NCCA device?

No, only you should use your NCCA device. As each device is linked to our platforms such as Teams and SharePoint, which has externally invited guests and access to sensitive documents as well as personal data, you should be the sole user of your NCCA device.

What can I use my NCCA device for?

Your NCCA device should only be used for official NCCA work. Streaming apps including social video conferencing apps should be used on personal devices only and your NCCA device should not be used for this. Downloading of non-work-related software can lead to security issues which, in turn, could contribute unintentionally to data breaches. With this in mind, please use NCCA devices solely for NCCA work.

Where can I save my work at home?

Any NCCA files should be stored in your NCCA OneDrive, on SharePoint or on MS Teams depending on which is most suitable for the material in question. Please avoid saving files to your desktop or to storage devices. The exception to this is multimedia work.

I need to work on posted and/or printed paperwork at home. What is the best way to do this from a data protection perspective?

Where possible, avoid bringing home paperwork or printing NCCA-related documents at home. If you do need to bring documents home, it is advisable to scan the documents to a PDF, store these files in your OneDrive and delete them once you are finished working on them. Any documents that are brought home in hard copy need to be stored in a secure space. This is especially important where the documents/papers contain personal data belonging to NCCA staff and/or others. Where home printing is necessary, you must ensure that printed material is held securely and returned to the office for filing or shredding.

Do I need to shut down my device when I am not using it?

Avoid leaving NCCA devices open and unattended. If you are leaving your device for a period of time, put the device to sleep or lock the device using the combination of Alt+Ctrl+Del. If you have finished using the device on that day, shut it down and store it away safely.

What are my options for video conferencing?

Every staff member has access to Microsoft Teams for internal video conferencing and external video conferencing. For larger meetings, where Microsoft Teams may not be suitable, there are now two separate Zoom accounts – one for post-primary and one for early childhood and primary. When setting up a video conferencing meeting, these are the only two platforms that should be used. During the video conference, ensure that you are the only visible person on the screen from your device. Depending on the sensitivity of the meeting, if at any time you feel you have insufficient privacy to contribute to the meeting, for example, if someone else needs to share the room with you at that time, please let the meeting convenor know that you may not be able to participate in the meeting.

Appendix C: Data Subject Access Request Policy

Introduction

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

- comply with our obligations under GDPR, and in particular, to respond in a timely and appropriate manner to DSARs;
- 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 and parents/guardians of children who have been recorded by the NCCA or have had their written work reproduced and published. This includes

- Video recordings
- Audio recordings
- Photographs
- Reproduction of hand-drawn and written work.

This media content is stored by the NCCA, edited into publications used to support the work of the NCCA, presented at NCCA events, and published on the organisation's websites.

The policy is also for DSARs from

- current and past employees either permanent or temporary
- current and past contractors
- current and past commissioned staff
- current and past Council members, members of subject or development groups
- 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 the 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 you originally collected or processed it for
    - If you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent.

Data Subject Access Request (DSAR)

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 F).

In the event that a Data Subject Access Request 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. The NCCA will not provide personal information via social media channels.

DSAR process

Step 1: Request for information

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

- Submit his/her request using the NCCA's Data Subject Access Request Form.
- Provide the NCCA with sufficient information to validate his/her 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, the 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 the NCCA.

However, the 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, the 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 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

The **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 data subject access request form and identification verification if necessary) the **Data Protection Officer** will notify the requestor that his/her 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

The **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

The **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). The 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 the **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. The 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 of the identity of the data subject making the request. In principle, the 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 six-month period of the original request will be considered a repeat request, and the NCCA will not provide a further copy of the same data.
- Publicly available information – The 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 – The 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 his/her DSAR is entitled to make a request for the outcome to be reviewed.

Appendix D: Data Subject Access Request (DSAR) Form

National Council for Curriculum and Assessment

Data Subject Access Request Form

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

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

Current 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 to indicate

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 information requested 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** **35 Fitzwilliam Square, Dublin 2** **DO2 KH36**	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 E: Sample Data Sharing Agreement between the National Council for Curriculum and Assessment (NCCA) and the [Name of organisation]

Purpose

[Brief overview of the personal data being shared and the purpose of the sharing.]

Terms of the Agreement

1. This Data Sharing Agreement covers the transfer of personal data as part of XXXXX from the NCCA to the [name of organisation] for the purpose of XXXXXXX.
2. Under this Agreement, the NCCA is the data controller, and both NCCA and [name of organisation] are data processors for the data in question.
3. The data will be transferred to [name of organisation] in a safe, secure manner agreed with the NCCA.
4. The following named individuals are designated as 'Points of Contact':
    a. **NCCA Contact**: name, XXXXXXX@ncca.ie / 087 XXX XXXX
    b. **XXXX Contact**: name, email / XXX XXX XXXX
5. Upon receipt or upon opening, the video files should be spot-checked to ensure that the data meets the pre-defined formats. If the files contain problems that prevent successful loading or reconciliation the parties will liaise to resolve any issues.
6. The data should not be adjusted without contact with the NCCA (the data controller).
7. The data will only be used by the [name of organisation] for the purposes outlined above.
8. The materials may not be transferred outside the [name of organisation] and/or uploaded to any website or social media platform other than those specified above.
9. The [name of organisation] will provide appropriate administrative, technical, and physical safeguards to ensure the confidentiality and security of the data and to prevent unauthorised use or access to it. For example, the video files must be stored on a device which is password-

protected. The NCCA may terminate this agreement if the necessary steps are not taken to safeguard materials.

10. If the [name of organisation] becomes aware of the theft, loss or compromise of any device used to transport, access or store the video files, or of the theft, loss or compromise of any of the data, they must immediately report the incident to all relevant internal parties and to the relevant NCCA party as named above.

11. The [name of organisation] will take any other reasonable measures to prevent any use or disclosure of the data other than as allowed under this Agreement.

12. This Agreement shall enter into force on the date that it is signed and shall continue in force for so long as the video files are shared between the parties, unless the parties agree in writing to terminate this Agreement or by the parties adopting a new agreement in place of this Agreement. The Agreement may be terminated by either party at any time for any reason upon 30 days' written notice. On the expiration or termination of this agreement, or on NCCA's request, the [name of organisation] will destroy all copies that have been made of the data which has been provided by NCCA and notify NCCA when this action has been completed.

13. This Agreement shall be governed by and construed in accordance with the laws of Ireland, and shall be subject to the exclusive jurisdiction of the Irish courts.

14. On behalf of both parties, the undersigned individuals hereby attest that he or she is authorised to enter into this Agreement and agrees to all the terms specified herein.

National Council for Curriculum and Assessment	[Name of organisation]
Party Transferring Data	**Party Receiving Data**
Date	Date

Appendix F: Privacy notice on the website of the National Council for Curriculum and Assessment – www.ncca.ie

This statement relates to the privacy practices in connection with this website. The NCCA is not responsible for the content or privacy practices of other websites. Any external links to other websites are clearly identifiable as such. Some technical terms used in this statement are explained at the end of this page.

General statement

The NCCA fully respects your right to privacy and will not collect any personal information about you on this website without your clear permission. Any personal information which you volunteer to the NCCA will be treated with the highest standards of security and confidentiality, strictly in accordance with the Data Protection Acts.

If you require further information related to data protection and www.ncca.ie you can contact the NCCA's Data Protection Officer at dpo@ncca.ie

Collection and use of personal information

The NCCA does not collect any personal data about you on this website, apart from information which you volunteer (for example by e-mailing us or by using an online survey or feedback form). Where you voluntarily provide personal information in response to a questionnaire or survey, the data will be used for research or analysis purposes only. Any information which you provide in this way is not made available to any third parties and is used by the NCCA solely for the purpose for which you provided it.

Collection and use of technical information

This website does not use cookies, apart from temporary 'session' cookies which enable a visitor's web browser to remember which pages on this website have already been visited. Visitors can use this website with no loss of functionality if cookies are disabled from the web browser.

Technical details in connection with visits to this website are logged by our internet service provider for our statistical purposes. No information is collected that could be used by us to identify website visitors. The technical details logged are confined to the following items:

- the IP address of the visitor's web server
- the top-level domain name used (for example .ie, .com, .org, .net)
- the previous website address from which the visitor reached us, including any search terms used
- clickstream data which shows the traffic of visitors around this web site (for example pages accessed and documents downloaded)
- the type of web browser used by the website visitor.

The NCCA will make no attempt to identify individual visitors, or to associate the technical details listed above with any individual. It is the policy of the NCCA never to disclose such technical information in respect of individual website visitors to any third party (apart from our internet service provider, which records such data on our behalf and which is bound by confidentiality provisions in this regard), unless obliged to disclose such information by a rule of law. The technical information will be used only by the NCCA, and only for statistical and other administrative purposes. You should note that technical details, which we cannot associate with any identifiable individual, do not constitute "personal data" for the purposes of the Data Protection Acts.

Glossary of technical terms used

web browser

The piece of software you use to read web pages. Examples are Microsoft Internet Explorer, Netscape Navigator and Opera.

IP address

The identifying details for your computer (or your internet company's computer), expressed in "internet protocol" code (for example 192.168.72.34). Every computer connected to the web has a unique IP address, although the address may not be the same every time a connection is made.

cookies

Small pieces of information, stored in simple text files, placed on your computer by a website. Cookies can be read by the website on your subsequent visits. The information stored in a cookie may relate to your browsing habits on the web page, or a unique identification number so that the website can "remember" you on your return visit. Generally speaking, cookies do not contain personal information from which you can be identified, unless you have furnished such information to the website.

Appendix G: Consent documentation

Project identifier no:

Consent form for children's participation (TEMPLATE)

Dear Parent/Guardian,

The National Council for Curriculum and Assessment (NCCA) advises the Minister for Education and Skills on curriculum and assessment for early childhood education, primary and post-primary schools. At present…(1).

-

What material will be gathered and how will it be used? (2).
_____ (Setting's/School's Name) is taking part in ….

- Your child's feedback may be used .....
- Your child's photograph may be used ….

Your child can stop taking part in the project at any stage. Your child's name will not be used in the published material.

What are your rights regarding personal data? (3).
You and your child have the following rights, in certain circumstances and subject to applicable exemptions, in relation to the personal data we hold:

- the right to access the personal data and information about our processing of that personal data
- the right to require us to correct any inaccuracies in the personal data
- the right to require us to erase the personal data
- the right to request that we no longer process the personal data for particular purposes
- the right to object to our use of the personal data or the way in which we process it.

Please note that to help protect your privacy and that of your child, we take steps to verify your identity before giving access to personal data.

NCCA will hold the photos/videos/written material for six years after which it will be deleted. You may, at any time, request that we remove any image/video your child appears in during these six years by contacting NCCA's Data Protection Officer at dpo@ncca.ie or by phoning 01 661 7177 or by writing to Data Protection Officer, NCCA, 35 Fitzwilliam Square, Dublin 2, D02 KH36.

Child Protection and Safeguarding is a core objective and priority of the NCCA. NCCA is committed to maintaining the highest standards of child safeguarding in line with relevant legislation and best practice. The NCCA's Child Safeguarding Statement is available to view here.

Please contact _____, NCCA, at _____@ncca.ie or 01 661 7177 if you would like more information about this project. (4).

Thank you for taking the time to read this letter.
Kind regards,

_____
Education Officer's name, Education Officer, NCCA

Consent form for children's participation: Parents'/Guardians' Copy

Please keep this form for your own records and return the one below to

_____ (practitioner's/teacher's name).

I give consent to the NCCA to ……. from _____ (child's/student's name). (1).	☐ Yes, I give consent. ☐ No, I do not give consent.
I give consent to the NCCA for ……(2).	☐ Yes, I give consent. ☐ No, I do not give consent.

Signed: _____ (Parent/Guardian) Date: _____

Home address:

_____

Setting/school name and address: _____

(The addresses help us to verify who you are if you ask us for your personal data which we hold.)

_____ (child's/student's name) agrees to take part in the NCCA's work.	☐ Yes ☐ No
Where possible, child/student can sign below if he/she agrees to take part in the NCCA's work. Child's/student's signature: _____	

Thank you for allowing your child to be involved in this important work.

Project identifier no:

Consent form for children's participation: NCCA's copy

This copy will be kept by the NCCA for its own records.

I give consent to the NCCA to …… from _____ (child's/student's name).	☐ Yes, I give consent. ☐ No, I do not give consent.
I give consent to the NCCA for ……..	☐ Yes, I give consent. ☐ No, I do not give consent.

Signed: _____ (Parent/Guardian) Date: _____

Home address:

_____

Setting/school name and address: _____

(The addresses help us to verify who you are if you ask us for your personal data which we hold.)

_____ (child's/student's name) agrees to take part in the NCCA's work.	☐ Yes ☐ No
Where possible, child/student can sign below if he/she agrees to take part in the NCCA's work. Child's/student's signature: _____	

Thank you for allowing your child to be involved in this important work.

Guidelines for using the Consent Form

Pages One and Two: Cover Letter

The first two page of the consent form provide a cover letter that should be included with every project for which consent is sought. Much of the text of the letter is generic and may be used across projects. However, where text specific to projects needs to be included the numbered instructions below provide guidance for adapting the template to the specific requirements. The numbered instructions refer directly to the numbers within the template.

1. The Education Officer provides a clear, brief outline of the specific project and a precise description of what consent is being sought for.
2. This section of the consent form addresses the specific project being undertaken and how data will be used by the NCCA.

   It is important that participants are made aware of exactly what information will be gathered and how it will be used. All future uses of data must be explicitly documented in the letter. If NCCA intends to use the data for more than one purpose this must be made clear. It is recommended that bullet points be used in this case for clarity.
3. This section provides an overview of the rights of participants and their parents and applies to all projects for which the NCCA will seek consent.
4. The contact details of the Education Officer leading the specific project need to be included in this section.

Page Three: Consent form for children's participation: Parents'/Guardians' Copy

Page three provides a template of the consent form for parents/guardians. Parents/guardians will keep a record of this consent form. As with the letter much of the text of the form is generic and may be used across projects. However, where text specific to projects needs to be included the numbered instructions below provide guidance for adapting the template to the specific requirements.

1. In this box NCCA outlines what data it intends to gather and seeks consent to gather this data, e.g. photographs, written feedback, videos etc…If the NCCA intends to gather data in more than one format a new box must be created for each separate format.
2. In this box NCCA outlines how it will use the data and seeks consent to use this data, e.g. on the websites, in support material on the website, in presentations etc…Again, if NCCA intends to use data in multiple formats more boxes will be required seeking consent for data to be used in each format.

Page Four: Consent form for children's participation: NCCA's copy

Page four provides a template of the consent for NCCA's records. This is a replica of the form that parents/guardians will keep and, therefore, this form must be adapted in precisely the same way.

Please see sample consent form below for further guidance.

Appendix H: Sample letter used to provide information relating to data protection

Project identifier no:

Sample letter for the consent form for children's participation

Dear Parent/Guardian,

The National Council for Curriculum and Assessment (NCCA) advises the Minister for Education and Skills on curriculum and assessment for early childhood education, primary and post-primary schools. At present, the NCCA is developing the Primary Language Curriculum for 3rd to 6th class in primary schools. As part of this work, we are gathering feedback on a draft of the curriculum. We wish:

- to gather children's feedback on language learning (English and Irish).
- to gather photographs of language lessons in classrooms.

What material will be gathered and how will it be used?

_____ (Setting's/School's Name) is taking part in the work on the language curriculum. We will be visiting the setting/school on 6th June, 2018. During our visit we will talk to children and gather written feedback on their experiences of language learning in school. We will also take photographs. The NCCA would be delighted if your child would take part in this project.

- Your child's feedback may be used in the report on the draft curriculum. This report will be published on the NCCA's website at www.ncca.ie.
- Your child's photograph may be used in the report.
- Your child's feedback and/or photograph may be used in NCCA presentations on the report.

Your child can stop taking part in the project at any stage. Your child's name will not be used in the published material.

What are your rights regarding personal data?

You and your child have the following rights, in certain circumstances and subject to applicable exemptions, in relation to the personal data we hold:

- the right to access the personal data and information about our processing of that personal data
- the right to require us to correct any inaccuracies in the personal data
- the right to require us to erase the personal data
- the right to request that we no longer process the personal data for particular purposes
- the right to object to our use of the personal data or the way in which we process it.

Please note that to help protect your privacy and that of your child, we take steps to verify your identity before giving access to personal data.

NCCA will hold the photos/videos/written material for six years after which it will be deleted. You may, at any time, request that we remove any image/video your child appears in during these six years by contacting NCCA's Data Protection Officer at dpo@ncca.ie or by phoning 01 661 7177 or by writing to Data Protection Officer, NCCA, 35 Fitzwilliam Square, Dublin 2, D02 KH36.

Child Protection and Safeguarding is a core objective and priority of the NCCA. NCCA is committed to maintaining the highest standards of child safeguarding in line with relevant legislation and best practice. The NCCA's Child Safeguarding Statement is available to view here.

Please contact XXX XXX, NCCA, at XXX.XXX@ncca.ie or 01 661 7177 if you would like more information about this project.

Thank you for taking the time to read this letter.
Kind regards,

_____

xx
Education Officer, NCCA

Appendix I: NCCA's Data Breach Policy

Introduction

The National Council for Curriculum and Assessment (NCCA) is a statutory agency under the aegis of the Department of Education and Skills (DES). The NCCA advises the Minister on curriculum and assessment for early childhood education, primary and post-primary schools. The NCCA strives to fulfil the requirements of the Data Protection Bill 2018, the General Data Protection Regulation 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 General Data Protection Regulation (GDPR) introduces 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.

The 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 act 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 the 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 the 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 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 great 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 J: NCCA's Data Breach Register

Pro forma for reporting Data Breaches—for NCCA's Register

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.

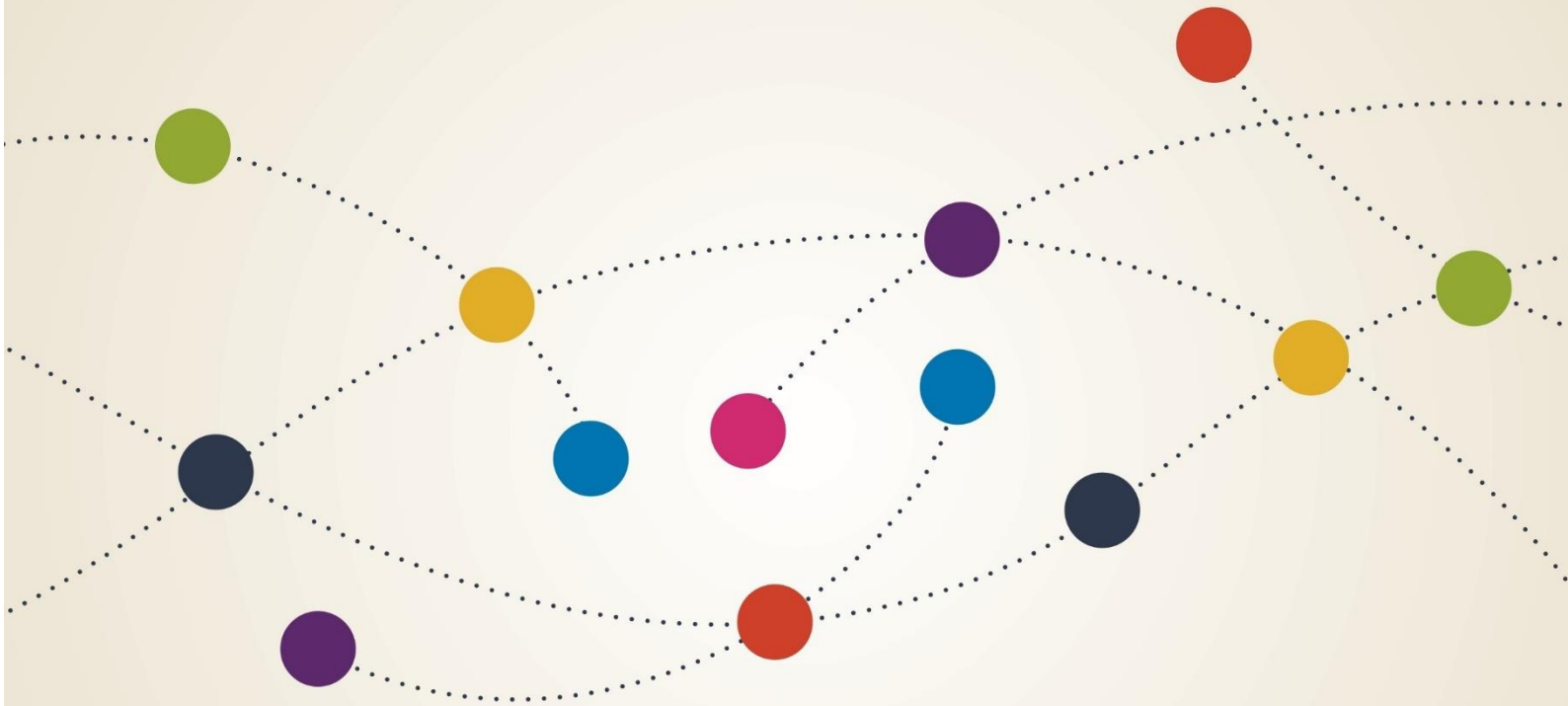
Date(s) of the Personal Data Breach	
Time of the Personal Data Breach	
Date and time the breach was discovered	
Name of person who discovered the breach	
Contact details of the person who discovered the breach	
Brief description of the breach	
Number of data subjects affected, if known	
Estimated level 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 of person receiving the report

_____ Signature	_____ Signature
Date _____	Date _____
Contact details of person reporting the breach	Action taken
	Date of action

****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