THE CHILDREN'S COMMISSIONER:
DATA PROTECTION POLICY

THE CHILDREN'S COMMISSIONER:
DATA PROTECTION POLICY

Introduction

The Children's Commissioner's Office ('CCO') gathers, holds, analyses and uses substantial amounts of personal data in discharging its functions, [ICO Registration number Z1102328]. The CCO is a data controller for that personal data. It is required to comply with the General Data Protection Regulation ('GDPR') and the Data Protection Act 2018 ('DPA'). This document outlines how the CCO seeks to ensure compliance with that legislation.

This document, alongside the Information Asset Register and related documentation, forms the CCO's records of processing for the purposes of Article 30 GDPR and its relevant policy document for the purposes of Schedule 1 DPA. This document will be reviewed annually to ensure that it contains an adequate and up-to-date record of the CCO's processing activities.

The principles set out in this document are mandatory for all CCO staff, temporary staff, contractors, partners and collaborators.

Queries and concerns from any data subject relating to the use of personal information should be raised with the CCO's information governance lead in the first instance: Info.REQUEST@childrenscommissioner.gov.uk. Nevertheless, all subjects are free to raise these verbally, in person, over the phone, or in writing.

The CCO has a designated Data Protection Officer ('DPO') who is responsible for overseeing the CCO's compliance with data protection duties. The role is provided by **TIAA Ltd** and **Jonathan Gladwin** is the named DPO. The DPO's contact details are:

OCC.dataprotectionofficer@childrenscommissioner.gov.uk

Personal data processed by the CCO

Personal data is information that relates to a living individual who could realistically be identified either from that information itself, or (where the data appears to be anonymised) by combining that information with other available information to establish the identity of the relevant individual. It may

also include data concerning someone who is deceased if that contains associative characteristics for a living person.

Where there is no realistic risk of any individual being identified from a set of information, it will not be personal data and will not be subject to the data protection duties outlined in this policy. For example, statistical data will often not be personal data, unless very small numbers of individuals are being referred to, multiple characteristics, or contextual information is provided with this data. In such cases, there may be risks of individuals with specific knowledge being able to discern whom those low numbers relate to.

'Special category' personal data (formerly referred to as 'sensitive personal data') is a distinct and more sensitive sub-category of personal data. It is defined as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" (Article 9(1) GDPR). Disability, maternity and paternity, and trans identity are included within this definition. While Criminal records information, (including allegations) is not part of special category data it should be treated with similar regard and can only be handled under strict conditions.

The primary categories of personal data processed by the CCO are as follows:

Information about the cases of particular identified children.

- Data Processed (May include): Name, date of birth, address, demographic information (including ethnicity and religion in some cases), health data where relevant, narrative information about circumstances and experiences, notes of interviews with children.
- Collected By : Help at Hand staff, policy and public affairs staff, qualitative researcher staff, the Children's Commissioner and her senior management team.
- Reason for Processing: providing advice and assistance to children in the care system and making representations to local authorities on their behalf, analysing policy and practice issues relating to vulnerable children, producing qualitative analysis, informing the Children's Commissioner and her staff about the experiences of children in the care system, in institutional care or in other situations of vulnerability.
- Data Shared with: Children's Commissioner Staff, This information is sometimes shared with external parties in the following circumstances: with the child's consent, with local authorities

in order to fulfil the CCO's statutory responsibility to provide advice and assistance to children in the care system. We do not provide information about particular identified children to any other external parties. If required to by law we may need to supply information to Law Enforcement Agencies or courts such as police forces and the National Crime Agency. We may supply information to prevent or assist in the detection of crime or as part of exercising or defending legal claims.

- Lawful Basis of Processing: Public Task (Children Act 2004)
- Retention Periods: are listed in the Information Asset Register [IAR]

Information about the family members/carers of particular identified children.

This information will typically include: identification of social workers or other responsible local authority staff, identification of staff in institutions where children are accommodated, location of children's homes or other institutions in which children are accommodated, information reported to CCO by members of the public which may include any of the above and other information such as details of school, health service or other local authority staff, cases of particular identified children. This information will typically include: name, date of birth, address, demographic information (including ethnicity and religion in some cases), health data where relevant, narrative information about circumstances and experiences, notes of interviews with children, etc.

- This information tends to be obtained by: Help at Hand staff, policy and public affairs staff and qualitative and quantitative researchers, the CCO helpline staff.
- This information tends to be used for: providing advice and assistance to children in the care system and making representations to local authorities on their behalf, helping to inform policy analysis, research with children to show their experiences of living with particular vulnerabilities.
- This information is sometimes shared with external parties in the following circumstances: with the child's consent, with local authorities, in order to fulfil the CCO statutory responsibility to provide advice and assistance to children in the care system, Ofsted, Care Quality Commission.

CCO does not provide information about particular identified children to any other external parties. Any external use of Personal data must be signed off by the Children's Commissioner or, the person she has nominated in the event of her absence, with due regard to this policy.

Any information which could lead to the identification of an individual person or institution should be anonymised prior to being included in any report, publication or external sharing of findings.

Information about CCO staff

This information will typically include: name, address, date of birth, employment record, references, CV, pay details, DBS confirmations, training history, relevant sickness records and appraisal records.

- This information tends to be obtained by: business services.
- This information tends to be used for: staff management.
- This information is sometimes shared with external parties in the following circumstances: for a reference (dates of employment, job title, salary and reason for leaving); for pension, HMRC and National Insurance; as part of an employment tribunal claim.

Data from the website

This information tends to be email addresses provided in order to sign up to the Children's Commissioner's newsletter. These emails are not shared or used for any other purpose.

A child might potentially be identifiable from quantitative data obtained by the Children's Commissioner analysts, for instance that relating to children in in-patient mental health care. Analysts and CCO staff will not share such data externally where it is possible to identify any individual child from it. The threshold for suppression of data (to avoid disclosure) will be taken on a case-by-case basis depending on the level of detail of the information being presented. Where the data has been provided by another public body, e.g. DfE or NHS Digital, their statistical suppression rules will be incorporated into the suppression decision.

From the above list, the types of Special Category personal data that are processed by the CCO include, but are not limited to:

- Health and social care data relating to children
- Racial or ethnic origin data
- Religion and philosophical belief
- Data relating to sexual activity, in particular sexual abuse of or by an individual
- Data relating to sexual orientation or trans identity

Information Asset Register

All Personal and Special Category personal data must be recorded by staff in the Information Asset Register (IAR) [located in shared folders, under corporate Information, Information Security]. This provides the details of the Information Asset Owner, those persons entitled to view the data, specification of disposal schedule and risk reviews undertaken or planned.

The IAR will be reviewed every three months by the DPO and the senior information risk owner [SIRO] to ensure it is up to date and that data are being held appropriately with risks being properly recorded and managed.

Below is a summary of the legal bases used by the CCO. These are provided specifically against each processing activity in the asset register.

a. Article 5(1)(a) GDPR requires the CCO to meet one of the lawful processing conditions in Article 6 GDPR, i.e. to specify the grounds on which it is allowed to process personal data. For special category personal data, a condition from Article 9 GDPR must also be met.

b. The CCO bases its processing of personal data on condition 6(1)(e) from Article 6: processing is necessary for the performance of a task carried out in the public interest. The CCO processes personal data in furtherance of her statutory functions (The Children's Act 2004, in particular sections 2, 2B, 2C, 2D, 3 and Schedule 1) which are conferred and discharged in the public interest.

c. The CCO bases its processing of special category personal data on conditions 2 and 9 from Schedule 1 to the DPA (which sets out how the conditions in Article 9 GDPR apply in the UK). Those conditions apply where processing is necessary for health or social care purposes (condition 2) or for the exercise of a protective function (condition 9).

d. The CCO's processing is 'necessary' for the purposes referred to in the relevant conditions: it could not realistically or effectively discharge its statutory functions without processing this personal data and special category personal data.

e. The CCO is unable to rely on individuals' explicit consent for its processing of their personal data. It is likely that there would be an actual or perceived imbalance of power between the CCO and data subjects. In every case, this would not be practicable because:

- Personal data is sometimes shared with CCO by external individuals without the consent of the data subject. In addition, on rare occasions, where it contains safeguarding concerns, the CCO is then obligated to pass this information to relevant authorities;
- CCO processes data relating to highly vulnerable children and children in state institutions whose meaningful full consent would be impossible to obtain;
- CCO processes quantitative data, for instance in relation to children in inpatient mental health facilities, where identification of those children might theoretically be possible but where in practice CCO would not seek to identify them.

How personal data is used and managed in practice

Personal data is obtained by CCO through interviews, focus groups and surveys; calls from children and young people; information provided by email or telephone from external people concerned about a child, data requests and administrative data.

Storage and Use

All electronically held Personal data should be held in the CCO area of the Department of Education ('DfE') encrypted system, which is only accessible through personally issued password-protected devices on personal password-protected accounts through secure connections.

Special Category and/or Personal quantitative data must be stored under restricted conditions; password protected, in a restricted folder, or both. The DfE IT system follows Cabinet Office Guidance on Information Security and ISO/IEC 27000:2014. Electronic data that is Personal and/or Special Category should only be seen by those with a reason to see it, with these people being recorded in the IAR.

A suitable Shared Area on the DfE network must be identified and created prior to the storage of Personal data. The Shared Area should only be accessible to members of staff who have been named as having access rights to the data in question. This may or may not be the same as the set of staff members involved in the project or piece of work for which the data is required.

- If an existing Shared Area provides the desired access/security level, then it suffices to create a new folder within that Shared Area.

- If no existing Shared Area provides the desired access/security level, then a new Shared Area must be created. This cannot be located within any other existing Shared Area. A request must be logged with the IS Helpdesk to create the new Shared Area.

In the event of the DfE not providing or being delayed in providing a new Shared Area, Personal Data will be stored using appropriate technical and organisational methods to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Files containing Personal and/or Special Category data stored in an MS Office format should remain encrypted with a password. It may not be possible to encrypt files stored in other formats (e.g. statistical software packages), either because the function does not exist or because doing so would prevent the file being processed by the statistical software.

Paper and hard copy data

In some isolated instances evidence requested via the call for evidence and data requests may be provided in hard copy, contrary to guidance. In this event the evidence should be scanned using the CCO's Printer which is linked to the DFE secure electronic network and sent to the secure mailbox. The hardcopy should then be disposed of using the secure confidential waste facility and the above steps followed. Should this not be possible immediately the material should be stored within the secure lockable storage cabinet and above process followed at the earliest opportunity.

Hardcopy Personal data which exists in the form of notes from interviews or visits to institutions in which children are accommodated, or from notes made for instance during telephone calls, should be transcribed and stored electronically and securely. Any hardcopy Personal data which is to be stored over an extended period should be stored in a specified locked and secure storage cupboard, within a lockable room with restricted access in Sanctuary Buildings, where entry to the building is restricted to staff and registered visitors.

Staff conducting field visits and interviews should take care not to include in notebooks any personally identifying information about any subject under the age of 18. Staff should assign a number to signed consent forms e.g., 001 and use this number for any notes made from the interview or focus group. Once interviews and notes are transcribed onto the electronic system, the paper copies should be destroyed in the secure waste bin.

When working from home, staff should continue to follow secure desk policy and the data protection policy regarding the storage of hardcopy personal sensitive data. Following transcription of notes,

notes should be stored safely, for example in a designated notebook or folder, until they can be taken to the office to be disposed of in the secure waste bin. Staff should take care to ensure that personal sensitive hardcopy data is not lost while working from home and store in a drawer or cupboard, taking reasonable care to request that other members of the household do not access the information.

Emails

Personal data should only be e-mailed unencrypted between gov.uk/nhs.net e-mail accounts.

Information should only be emailed outside trusted networks where there is a compelling business need approved by the Information Asset Owner. This approval will also need to consider the appropriateness of the recipient's email security arrangements to protect the data at rest, once received.

If Personal data needs to be e-mailed to a non-PSN/.gov e-mail account the data should be shared using Egress switch which provides secure transfer of data. Alternative secure transfer systems, such as WinZip or Citrix may be used occasionally when working with external contractors. Before a transfer method is agreed the SIRO will advise on whether the method is appropriate and conforms to the guidance set out in this policy.

Egress or WinZip will not be an appropriate transfer method in all instances, particularly where information needs to be conveyed to young people through Help at Hand. In this instance, the information can be shared as a password protected document (.xlsx, .docx or .pdf). The password shall be provided to the recipient by another form of communication. The person receiving the data shall be made aware of the importance of protecting the data once received.

Use of laptops

Any access, collation and analysis of Personal data undertaken by relevant CCO staff should only be done via their specific encrypted laptop provided by the CCO's approved IT provider, unless the data is to be hosted in another institution such as a data warehouse. Unless, no other option, Personal data should not be saved directly onto the hard drive of the laptop, nor should other CCO staff members/ persons be allowed access to it. In the event that a laptop is lost or stolen, compliance with the CCO's loss of information, data and equipment policy should be put into action. Should the laptop need replacing or transferred to another member of staff within the CCO or DFE then arrangements need to be made with IS Support to ensure that all content on the hard drive is securely erased in line with Information Assurance Standard (IAS) 5.

Recording devices

All audio or visual data should be recorded on encrypted digital recorders that allows for audio files to be password protected and stored securely. Following this, audio recordings should be uploaded and stored securely in a restricted folder. All visual data should be recorded onto SD cards using recording devices with this functionality. All recording devices/recordings/SD cards should be logged on the IAR and should be stored in the secure lockable cupboard when not in use. Once the audio/visual data has been transferred, the content should be deleted. At the culmination of the project the SD card should also be destroyed using the secure confidential waste facility.

Privacy Filters should also be attached to any monitors linked to IT terminals which will be used to handle Personal data. These can be ordered via the CCO Business services team.

When conducting interviews remotely sessions can be recorded either using the online service provider's recording functionality or using a DfE allocated phone using the Samsung Voice Recorder App. When recording interviews using the online service provider's recording functionality the recording will be saved to a DfE laptop and not to the service provider's 'cloud' storage. When recording using the Samsung Voice Recorder App recordings will be immediately transferred to a DfE laptop electronically and then deleted from the phone.

Mobile Phones

Names and contacts of CCO stakeholders should only be stored on DfE allocated encrypted laptops or mobile phones. Personal phones should not be used for storing stakeholder contacts. **Receipt of Information from External Sources**

All data requests using formal powers or otherwise involving the transfer of Personal data must be accompanied with clear guidelines which set out the process by which the data can be transmitted to the CCO, with clarity on how the resulting data will be stored. This guidance must set out:

a) **Encryption methods and instructions:**

Prior to transfer, organisations and individuals providing Personal and/or Special Category data to CCO should encrypt data files individually with a password, or store the data files in a password protected compressed folder/ZIP file. The password(s) should then be passed to the CCO via a separate method of communication to the one used for data transfer (e.g over the phone or by SMS).

b) **Data transfer:**

In many cases, the organisation providing electronic data to CCO will have its own secure data transfer system based on a web or FTP interface, and CCO will be required to use that system. This would be

the case when CCO requests sensitive administrative data extracts from a government department or agency.

Where such systems do not exist, CCO or the organisation providing data to CCO will need to devise a transfer method that provides adequate security.

- External organisations may send data to CCO via government approved secure email systems including .gsi and .pnn email systems (if in use). The data should still be encrypted prior to transfer as above.
- If external individuals do not have access to a secure email account, the data must be encrypted prior to transfer as above.
- Where CCO uses secure online surveys to receive data (e.g. Smart Survey), CCO will request that survey participants encrypted the data prior uploading it.

Acknowledgement of receipt of Personal Data:

All Personal data submissions should be acknowledged with a response by the CCO. This should confirm that the data has been received and, if required, arrangements for the safe receipt of the password should be made.

Logging of evidence and removal from transfer medium:

On receipt of Personal Data electronically and following decryption (if necessary) the data should be transferred into a designated secure folder and stored according the instructions above. An entry should be made in the IAR providing the details of the data received and its storage location on the network. If the data was received via email, the original email should then be deleted from the secure mailbox and the trash folder deleted.

Checking the evidence:

Once the data has been transferred to the secure folder and password protected a review must be performed of the content. If information has been provided that was not requested or is not necessary (e.g. provided full personal identifiable data) then this should be deleted and the originator notified.

External disclosures and information-sharing

In order to provide the assistance and representations required of them, Help at Hand may need to disclose Personal Data to relevant local authorities, OFSTED and/or other institutions/organisations. Where possible this is always done with consent. However, for the reasons set out earlier in this document, explicit consent is not always practicable.

Such external disclosures will normally by made by Help at Hand staff in e-mails, with due regard to this policy.

Identifiable information about a child is only ever disclosed in CCO communications, beyond Help at Hand, with the written agreement of the Children's Commissioner, or the person she has nominated in the event of her absence.

How the CCO ensures that confidentiality is respected

When CCO staff obtain information from children through interviews, children/their parents and guardians are told, in writing where possible but otherwise orally, that information they provide to the CCO will be used to inform policy-making and the preparation of reports, but that no child will be identified in any report.

When Help at Hand staff obtain information from or about children, where possible the children, their parents/carers will be told, in writing where possible but otherwise orally, what their information will be used for and that it will only be shared with necessary authorities, as agreed in advance and in accordance with Help at Hand protocols.

CCO ensures that these duties of confidence are respected by training staff in data protection procedures and making clear in the staff handbook that information may only be used for designated purposes and not disclosed externally otherwise than by agreed procedures.

Staff who fail to follow these policies and guidelines may be disciplined, in accordance with CCO's Disciplinary and Grievance Policy, for failure to manage Personal Data in accordance with this policy. Unauthorised disclosure of Personal data may be considered gross misconduct. All consultants and contractors are also obliged to act in accordance with this policy. Staff who are concerned that an unauthorised disclosure may have taken place can report any such incident, in accordance with the Children's Commissioner's whistleblowing policy.

Transparency

The CCO has duties under Articles 12-15 GDPR to be transparent about how it uses personal data. It fulfils those transparency duties in the following ways:

1. When personal data is obtained from data subjects (children, their carers or families), they are provided with the following information if practicable and possible in writing, otherwise orally:
    - What Personal data about them is being processed, by whom and why;
    - That they have a right to see such data;
    - That, unless an exemption applies, they have the right to object to their data being processed, and the right to have it erased or corrected (if incorrect).
2. When personal data is obtained from other sources, the CCO explains through its online privacy policy how it obtains and uses personal data, the key points of which are as follows:
    - Any e-mail addresses provided via the newsletter sign-up will be used for the purpose of communicating newsletters from CCO.
    - Advice and information to users who fill in 'contact us' and Help at Hand forms.

    CCO will not share or pass on Personal data collected in this way unless there is concern for a person's safety, in which case CCO may need to pass on relevant details to the relevant authority.

    Any user providing Personal data has a right to see such data, have such data removed from CCO's database at any time.

    CCO's contact details are provided.

Retention periods

Unless there is lawful reason to retain Personal data for longer, (such reason to be identified in the IAR and the revised length of retention stated there), the following is a summary of the policies apply and specific retention policies for each piece of information will be detailed in the information asset register:

- Hard-copy Personal data is disposed of after one year of collection. This is done by Department of Education secure waste bins;
- Electronic Personal data is disposed after two years of collection. This is done by [explain process].

- Save, where information is relevant to an inquiry, when additional stipulations around retention may be set out as part of the ethical strategy/approval process and should be adhered to accordingly.

The IAR will enable these timeframes to be monitored and it is the responsibility of the DPO and the Information Asset Owner to ensure that data is disposed of in line with this policy.

The CCO's email retention and archiving policy is as follows:

- Information about employees is retained for six years after their employment ceases.
- Information about unsuccessful applicants will be retained for two years after the closing date of a post.

Data security

The CCO has duties under Article 5(1)(f) and Article 32 GDPR to ensure that it implements appropriate measures to ensure data security. It does so as follows:

- OCC has a Shared Services Agreement with DfE for the provision of its IT systems. DfE's Chief Information Security Officer has confirmed that its managed IT systems are developed, delivered and maintained under the DfE Information Security and Risk Governance framework, with senior oversight at both the Leadership team and the Audit and Risk Committee.
- Security assurance, executed through the Cyber and Information Security division, is provided across the DfE estate. Security controls are deployed at initial development and through the life cycle of services, such that appropriate and proportionate levels of risk are maintained.
- External assurance is further provided by an annual programme of independent audits executed by the Government Internal Audit Agency (GIAA) and the annual Cabinet Office Departmental Security Health Check.
- The CCO's Information Security Policies and Procedures provide guidance rules for the protection of information, both through electronic and physical controls. Compliance with these policies ensures that data does not leave CCO premises unnecessarily and sets out good practice for using laptops and other mobiles devices.
- No CCO data should be created, held or stored on non-CCO equipment nor should CCO data be transmitted to or stored in personal (non CCO) internet accounts unless previously agreed with the Children's Commissioner, or the person she has nominated in her absence.
- Staff training [see below]

International transfers

CCO does not transfer personal data outside the EU. Data processors/suppliers are required to seek written consent prior to so doing.

Staff training

The Children's Commissioner for England will provide for staff:

- Data protection training as part of the organisation's induction programme:
- Annual training: Responsible for Information- IAO Level 2 via civil service e-learning:
- Ongoing advice on data protection as needed from the DPO.

External processors

Article 28 GDPR stipulates the contractual provisions data controllers must have in place when using external data processors.

Almost all, if not all of CCO's analytical data processing is done in-house by CCO staff.

In the event of needing to use an external organisation to process Personal data, CCO uses recognised research consultancies with policies equal or equivalent to those specified here. Prior to the sharing of information CCO asks for a data handling/information security policy in advance for review. A data sharing contract is then drawn up covering, amongst other terms, what the data can be used for, how long it can be retained and how it should be stored and accessed to ensure proper compliance with GDPR and DPA.

CCO uses the services of the following data processors:

1. DfE IT services and support and secure waste disposal and shredding services. DfE will fully comply with GDPR in carrying out these service for CCO; and
2. Iron Mountain provide secure paper records storage. CCO will ensure that their contract with Iron Mountain fully complies with GDPR.
3. MyCSP provide pension services.
4. CS Resourcing provide an advertising forum for job vacancies.

Work with other data controllers

CCO does not routinely work in partnership with or share data with other organisations. CCO does regularly receive National Pupil Database extracts from DfE, through an MOU which both parties have signed (and which is available upon request). However, CCO does not share this data – or any other data – with other organisations.

Prior to the commencement of any joint project, a data sharing agreement will be drawn up setting out the respective responsibilities of the parties, with special care given to how the rights of the data subjects will be dealt with, in order to comply with Article 26 GDPR.

Compliance with individuals' specific rights under the GDPR

The GDPR confers specific rights on individuals, in particular:

Subject access (Article 15)

More information can be found in the Access to Records Policy

Right to request that personal data be rectified or erased (Articles 16-17)

- This is a qualified right and will be balanced against of the needs of the organization and the interests of the public as well as the requestor

Right to restrict or object to processing (Articles 18 and 21) needs of

- This is a qualified right and will be balanced against of the needs of the organization and the interests of the public as well as the requestor

Right to data portability (Article 20) i

- This only applies to data processed under consent or contract that has been provided by the subject themselves and processed by automated means.

Rights request can be received by any member of staff. They will pass this request on to the IG lead. If the requestor has already verified their identity the IG lead will write to the requester to notify them of the detail of the request. If Identity has not been verified then they will seek proof of identity before completing the request.

The time limit for the organisation to comply with or decline a request is normally one calendar month from the day after the request has seen received and identity verified. If the decision to decline the request has been made then the rationale for the decision must be provided to the requester along with information on how they can complain to the DPO and the ICO. In exceptional cases it is possible to request an extension of up to two months. If it becomes apparent that one month is not sufficient

to comply with the request then this must be communicated to the subject as soon as this is known and in any case within one month. Information about their rights to complain to the DPO and the ICO must be included with the extension request.

Rights requests must be balanced against the interests of the person, other individuals, the organisation, and the public.

Professional opinion would not normally be rectified or removed but may be updated with additional information including to the effect that the professional's opinion was incorrect.

Data protection impact assessments

The CCO is required under Article 35 GDPR to undertake a data protection impact assessment when a type of data processing is likely to result in a high risk to the rights of individuals. Given that the CCO works with sensitive information about children, it will consider undertaking such an assessment before commencing any major new projects (including significant new work streams or activities or types of analysis), new collaborations (with external organisations) or changes to its operations (including new IT systems). The information governance lead will ensure that an impact assessment is undertaken in accordance with Article 35 GDPR in such cases and that the Data Protection Officer is consulted as part of the process.

Procedure in the event of a data breach

Article 4 GDPR defines a 'personal data breach' as a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". The CCO is required under Articles 33 and 34 GDPR to report personal data breaches in certain circumstances. It will often be necessary to report a personal data breach to the Information Commissioner's Office. It will sometimes be necessary to report such a breach to the individuals whose data has been compromised.

All CCO employees and contractors must immediately alert their line manager and the DPO to any incident involving the loss of personal data, the sending of personal data to the wrong recipient or any other unauthorised access to personal data. A failure to report such incidents immediately can be a serious disciplinary matter.

In the event of a personal data breach, the information governance lead will consider the matter and in consultation with the Data Protection Officer will decide whether reports should be made in accordance with Articles 33-34 GDPR. They will also consider any appropriate remedial measures.

The decision to report will be taken by [insert role here, often the SIRO or IG Lead] and advice will be sought from the DPO. Various factors will be used to determine whether or not a breach should be reported to the ICO and these will include the number of people affected, the types of data involved, the likely impact on individuals and services, the probability of recurrence, and any mitigations in place.

Where information is available to contact affected subjects or their legal guardians the organization will do so in the event of a personal breach so long as doing so will not unduly increase the risks to those individuals or others.

Compliance with the principles in Article 5 GDPR

Article 5(1) GDPR sets out the key principles that must be complied with when processing personal data. Article 5(2) requires data controllers to be responsible for compliance and for demonstrating their compliance with those principles.

The CCO's compliance with those principles is demonstrated by the preceding sections of this policy. To summarise:

- Lawfulness, fairness and transparency: this policy explains how the CCO ensures that its confidentiality obligations are respected. It also explains the lawful processing conditions relied upon and the transparency measures implemented by the CCO.
- Purpose limitation: this policy explains the purposes for which the CCO processes personal data. It also explains how the CCO ensures that its confidentiality obligations are respected, i.e. how the CCO ensures that personal data is not used for any other purposes.
- Data minimisation: this policy explains how CCO staff are required to assess whether the information they record about cases is necessary. This discipline ensures that the CCO only processes personal data that it needs for discharging its functions. This also assists in ensuring that the CCO implements data protection by design and default in accordance with Article 25 GDPR.

- Accuracy: all CCO staff are responsible for ensuring that the personal data they record, store and use is accurate.
- Storage limitation: the CCO's retention policy is set out above.
- Integrity and confidentiality: this policy explains how the CCO ensures that its confidentiality obligations are respected. It also explains the CCO's data security and staff training measures.

Compliance with this policy

This policy will be communicated in training to all CCO staff.

As part of the annual review of the adequacy of this policy, the DPO will also undertake a proportionate audit of the CCO's processing of personal data in order to assess whether this policy if being complied with in practice. A report of that audit will be presented to the Audit and Risk Committee and will be retained on file.

Version control

Version	Description	Author	Comments
0.1	Draft policy	LF	
0.2	Reviewed by the Data Protection Officer	RB	Amendments made prior to review by ARC
0.3	Reviewed by the Audit and Risk Committee	ARC	21 November 2017
0.4	Edited in light of ARC comments and legal review	SG	
0.5	Reviewed by DfE Data Protection Officer	EW	Amendments made to reflect feedback
0.6	Information re DfE IT systems provided by DfE's Chief Information Security Officer	JG	Amendments made to reflect advice
1.0	Final policy	HC	January 2019
1.1	Update to Page 8/9 section 'emails'. Provide more detail of how data can be shared and protected when sharing via email.		
1.2	Update to Page 10 added section 'mobile phones'		
1.3	Update to section 'Recording Devices' to include remote interviewing. Updated 'paper and hardcopy data' section to link to secure desk policy and provide policy for managing paper records when working from home.		Comes into effect 20/05/20