

## COMDA-03-DATA PROTECTION

### 1 INTRODUCTION

- 1.1 This policy sets out how all staff and the Trust Board will ensure that personal and sensitive personal data of both students and staff is dealt with correctly and securely and in accordance with the General Data Protection Regulations (GDPR), and other related legislation.
- 1.2 The Trust processes personal data relating to students, staff, governors, visitors, and parents and is therefore a data controller.
- 1.3 In accordance with the regulations, the Trust is registered as a Data Controller with the Information Commissioner's Office (ICO). This is renewed annually.
- 1.4 The register is available to view here:  
[http://www.ico.org.uk/what we cover/register of data controllers](http://www.ico.org.uk/what_we_cover/register_of_data_controllers)
- 1.4.1 The Data Protection Act 2018 (DPA2018), and the General Data Protection Regulations (GDPR) establishes a framework of rights and duties which are designed to protect and enforce the privacy of personal data whilst also allowing for the lawful and appropriate use, sharing or transfer of this type of data.
- 1.5 The Regulations are underpinned by a set of six principles. The Trust is committed to following these principles as set out in this policy. The principles say that personal data must be:
  - Processed lawfully, fairly and in a transparent manner,
  - Collected for specified, explicit and legitimate purposes,
  - Adequate, relevant, and limited to what is necessary to fulfil the purposes for which it is processed,
  - Accurate and, where necessary, kept up to date,
  - Kept for no longer than is necessary for the purposes for which it is processed,
  - Processed in a way that ensures it is appropriately secure.

### 2 ROLE OF TRUST BOARD AND COMMITTEES

- 2.1 The Trust Board has overall responsibility for ensuring compliance with all relevant data protection obligations.
- 2.2 The Trust Board will appoint a named Trustee to be responsible for the strategic management of Data Protection and work the Trust's Data Protection Officer (DPO).

### **3 ROLE OF PRINCIPAL AND SENIOR LEADERSHIP TEAM**

- 3.1 The Principal acts as the representative of the Data Controller on a day-to-day basis.
- 3.2 The Principal will communicate with the Trust Board regularly on all matters related to data protection.
- 3.3 The DPO is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable. They will report directly to the Principal and Trust Board on any data protection issues or recommendations. The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO.
- 3.4 The DPO role is shared with SMBC's Information Governance Team.

### **4 DEFINITIONS**

- 4.1 **Personal Data** – Any information relating to an identified, or identifiable, living individual. This includes but is not limited to:
- Names,
  - Email addresses,
  - ID numbers,
  - Images,
  - It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity.
- 4.2 **Special Categories of Personal Data** – previously referred to as 'Sensitive Personal Data'; this includes information about an individual's racial or ethnic origin, political opinions, religious beliefs, and trade union memberships. It also includes an individual's genetic or biometric data (including fingerprints) and any data relating to an individual's physical, mental or sexual health.
- 4.3 **Processing** – Any automated or manual act involving personal data such as collecting, storing, altering, using, sharing/transporting, and destroying.
- 4.4 **Data Subject** – The individual whose personal data is being held or processed.
- 4.5 **Data Controller** – A person or organisation that determines the purposes and means of processing personal data.
- 4.6 **Data Processor** – A person or body that processes data on behalf of the data controller.
- 4.7 **Information Commissioner's Office (ICO)** – This is the statutory regulator for data protection and information processing.
- 4.8 **Data Protection Officer (DPO)** – the person at the Trust who manages and oversees data protection.

- 4.9 **Regulations/GDPR** – The General Data Protection Regulations which became law with the Data Protection Act in May 2018.
- 4.10 **On Site** – the Gipsy Lane campus, car parks, yards, fields and buildings. This specifically excludes Holly Lane.
- 4.11 **Off Site** - everywhere else.
- 4.12 **Subject Access Request (SAR)** – When a request is made to receive a copy of the personal data held and processed by the Trust. This has to be responded to within 15 working days of receipt and completed within one calendar month, unless it is particularly complex, or there are a number of requests, in which case up to an extra two months are permitted.
- 4.13 **Data Breach (DB)** - When personal data which the school controls is accidentally or unlawfully destroyed, lost, altered, disclosed, or accessed without authorisation. There are certain times when the significance of the data that has been breached has to be reported to the Information Commissioner’s Office within 72 hours of the breach being noticed. You are required to report DBs to the school’s Data Protection Officer as soon as possible, *within 24 hours of discovery of the DB*, and to complete all documentation with urgency.
- 4.14 **Freedom of Information Requests (FOI)** – When a person or organisation requests information about the data held by the Trust. The information requested is usually to be presented in the form of a summary (e.g., how many students continued to Key Stage 5 from Key Stage 4, what is the percentage of female students studying STEM subjects over the last 5 years etc.). The Freedom of Information Act (2000) states that requests must be complied promptly, within 20 working days.

## 5 STAFF

- 5.1 This policy applies to all staff employed by the Trust, and to external organisations or individuals working on our behalf (referred to as “Staff” for the rest of this policy). This includes supply staff and volunteers.
- 5.2 Staff and volunteers who do not comply with this policy will face disciplinary action.

5.3 All Staff are required to comply with this policy under the following circumstances:

- Collecting, storing, and processing any person's personal data,
- Informing the Trust of any changes to their personal data, such as a change of address,
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure,
  - If they have any concerns that this policy is not being followed,
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way,
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area,
  - If there has been a data breach or they have any concerns that there may have been a data breach,
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals,
  - If they need help with any contracts or sharing personal data with third parties.

## **6 STUDENTS**

- 6.1 This policy applies to all students who are educated by the Trust. External organisations who bring students to the school premises are requested to ensure that their students understand the purpose of this policy.
- 6.2 All students are required to comply with this policy. Those who do not comply with this policy will be managed according to the Behaviour Policy.
- 6.3 Students are required to assist the Trust in investigating breaches of this policy in order to ensure the safety of the Trust's community.

## **7 OF THE DATA PROTECTION ACT 2018**

### **7.1 Processing data fairly, lawfully, and transparently**

7.1.1 The Trust will inform students, staff, parents/carers, and any other data subjects why they need their personal data, how it will be used and with whom it may be shared. This will be done via Privacy Notice documents issued with the appropriate data collection form and also via the website where this is necessary.

7.1.2 The Trust will process personal data with regard to the conditions laid out in the GDPR and where appropriate consent will be sought.

7.1.3 The Trust will only process personal data lawfully.

### **7.2 Processing data for specific, explicit purposes**

7.2.1 Personal data held will only be used for statutory purposes as outlined in the Trust's Privacy Notice unless explicit and affirmative consent has been granted.

7.2.2 Data will only be shared with external parties where a statutory basis exists to do so, or we have acquired consent.

7.2.3 Where data is shared outside of the European Economic Area (EEA), including with cloud providers, checks will be made to ensure an adequate level of protection for that information and consent will be sought from those affected where required.

### **7.3 Processing data which is adequate, relevant and limited to only what is necessary**

7.3.1 The Trust will endeavour to collect enough personal data that is sufficient for the purpose and will not ask for more information than is necessary.

7.3.2 The Trust will regularly review data collection forms and will check personal data already held for missing, irrelevant, or seemingly excessive information.

### **7.4 Ensuring data is accurate and, where necessary, kept up to date:**

7.4.1 Data held by the Trust will be as accurate and up to date as is reasonably possible and steps will be taken to regularly check the accuracy of personal data held; an example is the annual data form issued to all parents to check all details are up to date.

7.4.2 If a student, member of staff, a parent or any other data subject informs the Trust of a change of circumstances or an error the relevant personal data will be updated as soon as is practicable.

### **7.5 Ensuring data is kept only for as long as it is required:**

7.5.1 The Trust will not keep personal data for longer than is necessary for the stated purpose(s). In order to ensure this, all information held and/or created by the Trust or held on its behalf will be retained according to timescales set out in the Trust's Data Retention Schedule.

7.5.2 The Trust will ensure that all personal data deleted or physically destroyed is done in a secure and confidential way.

- 7.6 Ensuring that the data is handled in such a way that ensures appropriate security, including data protection against unlawful or unauthorised processing, access, loss, destruction, or damage:
- 7.6.1 To prevent unauthorised/unlawful processing and accidental loss, destruction of, or damage to personal data the Trust will ensure appropriate security measures are in place to safeguard all personal data whether held in paper files, on a computer system, laptop or on portable media storage devices e.g., USB Memory Sticks.
- 7.6.2 Paper records and portable media storage devices must be kept in a locked room, cupboard, or drawer when not in use and only accessed by those authorised to see the information held on them. Portable media storage drives must have added encryption software as standard.
- Portable media storage drives which are being sent to external exam boards **cannot** be encrypted. The exam boards routinely reject encrypted portable storage drives.
- 7.6.3 Personal data held electronically is kept securely, is protected by passwords, and is only accessed only by those authorised to see the information held.
- 7.6.4 The Trust will avoid storing personal information on the hard drive of PCs or portable equipment and media, including, but not limited to, laptops, tablets, tablet PCs, netbooks, memory sticks, external hard drives, CDs, and DVDs, but where this is necessary the relevant equipment or portable media will always be encrypted. If it is necessary to take any of these assets outside of the on-site buildings, they will be protected in transit using the school-provided bags, they must not be left unattended and they must be stored securely.
- 7.6.5 Particular care must be taken when sending personal data via emails, faxes, and letters, etc. to use secure methods and only to confirmed addresses/numbers. School email may not be sufficiently secure. Data sent to external organisations via email must be encrypted using Barracuda. The recipient then receives an encryption link and can access the email via a (free) Barracuda account to enable access to the unencrypted message.
- Emails which are being sent to external exam boards **cannot** be encrypted. The exam boards routinely reject encrypted emails.

- 7.6.6 All breaches of this policy will be investigated and may be deemed to be a disciplinary matter.
- Staff must report actual or potential data breaches to the DPO immediately using the email [dataprotection@heart-england.co.uk](mailto:dataprotection@heart-england.co.uk)
  - Staff must complete the part 1 data breach form (COMDA-A03-02-Data Protection – Report Data Breach) as soon as possible. This must be within 24 hours of discovering the breach and must be emailed to the DPO immediately on completion.
  - The DPO must check the Data Breach form as soon as possible, completing the part 2 data breach form (COMDA-A03-03-Data Protection – Review Data Breach)
  - The DPO must pass the information onto the Principal/Trust Board as and when appropriate. High level concerns which will be passed onto the ICO must be managed immediately.
  - The DPO must update the log of Data Breaches to ensure completion of summarised records.
- 7.6.7 The Trust will ensure that any contractors who process personal information on the Trust's behalf will do so under clear written instruction and will have adequate safeguards in place to protect the information.

## **8 RIGHTS OF THE DATA SUBJECT**

- 8.1 The Trust will support the lawful specific rights of any person whose details are held/processed by the Trust, including:
- 8.1.1 To receive information about how the Trust is collecting their data about how it is used and processed,
  - 8.1.2 A SAR must be passed to the DPO immediately. The best way to make a SAR is described in COMDA-P03-1-Data Protection – Subject Access Requests, however, *all* forms of request (verbal, or written) must be passed to the DPO,
  - 8.1.3 Ask the Trust to rectify incorrect data,
  - 8.1.4 Have data erased,
  - 8.1.5 Stop, object, or restrict processing of their personal data, in the following circumstances:
    - Prevent use of their personal data for direct marketing,
    - Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them);
    - Challenge processing which has been justified on the basis of public interest.
  - 8.1.6 Be notified of a data breach (when their personal data has been passed on inappropriately to the wrong person),
  - 8.1.7 Data Portability (allowing data to be transferred for reuse for different services),
  - 8.1.8 Make a complaint to the ICO.
- 8.2 Individuals should submit any request to exercise these rights to the DPO.
- 8.3 If staff receive such a request, they must immediately forward it to the DPO.



## **9 EMAILS/COMMUNICATION OF SENSITIVE INFORMATION**

9.1 Personal information that is being communicated, by whatever method, needs to be looked after carefully,

- Paper based information must be kept safely, it must not be left unsecured or where other people, particularly non-staff, can come across it.
- Electronic information must be checked when there is no chance of it being viewed by non-staff. This requires vigilance when a staff laptop is connected to a projector.

9.2 Use of electronic communication must be categorised to enable quick analysis of its contents, regardless of the mechanism used for communication (e.g., MIS system, educational system, e-mail; all have the same constraints).

- All communications containing a direct reference to sensitive information about a student must have the subject BEGIN with the word CONFIDENTIAL.
  - When on site it is straightforward to use a setting of “Confidential,” this is optional,
  - When using Microsoft 365 it is not obvious. The subject content gives clear guidance.
- Staff must not view communications which are CONFIDENTIAL in front of other students.
  - These can be viewed when there are no students around e.g., before the working day, during social time and at the end of the working day.

9.3 Use of the Trust’s Safeguarding Management System must:

- Be managed by the DSL and the deputy DSLs,
- Only be displayed to those people who are directly involved in the care and support of the student,
- Only be accessed in a time and place where the data is kept safe from accidental viewing.



## **10 ISSUES SPECIFIC TO THE TRUST**

10.1 Consent: When a student is first registered to the Trust, consent for the following will be given by the student (16 and over)/parent:

10.1.1 Photographs/Recordings of students used in Trust publications, including those to be used in the local newspaper and letters,

10.1.2 Photographs/Recordings of students that are used internally by the Trust, for project work,

10.1.3 Photographs/Recordings of students, staff, and parents to be used on any web page.

The express consent of the students/parent or staff member must be received due to the potential of the image/recording being viewed worldwide, which may include countries without adequate protection of personal information.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

10.2 CCTV – Please see the CCTV policy COMDA-09-CCTV.

10.3 Displays of students' work.

10.3.1 Student work that is on display at a public venue (not the Trust premises) the personal data exposed must be kept to a minimum (e.g., First Name, possibly with Year Group).

10.4 Biometric Data

10.4.1 The Trust has notified parents about its use of an automated biometric (fingerprint) recognition system, which may be used when staff and students pay for food. Any further plans for biometric systems will be publicised before implementation.

10.4.2 Every person using the system must have consent for this to take place.

10.4.3 An alternative system is available for those people who do not want to use the biometric system (use of ID card).

10.4.4 Biometric data is a special category of personal data. Use of it is controlled by the Protection of Freedoms Act 2012.

## **11 COMPLAINTS**

11.1 These will be dealt with using the Trust's Complaints Policy.

11.2 Complaints relating to the way that the Trust handles data and information may be referred to the ICO however, they should be referred as follows:

11.2.1 To the Data Protection Officer, for investigation.

11.2.2 If the complaint applies to the DPO then it must be reported to the Principal.

11.2.3 If the complaint applies to the Principal, then it must be reported to the Chair of the Trust Board.

**12 AUTHOR**

12.1 The author of this policy is the Data Protection Officer. They should be contacted for any points of clarification or suggested future amendments.

**13 VERSION CONTROL**

<b>Policy Number</b>	COMDA-03
<b>Policy Name</b>	Data Protection
<b>Version Number</b>	04
<b>Publication Method</b>	External  A copy must be made available in U:\Staff Information\Policies\COMMunications and DAta Policies
<b>Approved by</b>	Full Trust Board
<b>Date of Approval</b>	February 2024
<b>Key changes since previous version</b>	1. Clarification of SAR process.
<b>Next review date</b>	February 2025



## PROCEDURE

### **COMDA-P03-1-DATA PROTECTION – SUBJECT ACCESS REQUEST**

#### **1 INTRODUCTION**

- 1.1 The Data Protection Act (2018) (DPA) requires all Data Processors to make personal data available to parents/carers/students on request, so that the records can be checked for accuracy and to ensure equality of access.
- 1.2 In addition, regulation 5 of the Pupil Information Regulations provides that the Trust must make a pupil's educational record available for inspection or provide a copy of the record within 15 school days of a parent/carer's/data subject's written request.
- 1.3 This procedure gives guidance on how to make a Subject Access Request (SAR). You need to be able to explain your relationship to the Data Subject.
- 1.4 For clarity:
  - SARs give specific information about a named person. If you want general information, which is available to anybody, on request then you need to make a Freedom of Information Request (FOIR). Please see the policy COMDA-10-Freedom of Information and it's procedure.
  - SARs may have parts of their content redacted (made impossible to read). This is because the contents must not identify anyone else's personal data.

#### **2 TASK DESCRIPTION**

- 2.1 All SARs must be passed to the Data Protection Officer (DPO) in the school. They do NOT have to be made using this form, but it is helpful if they are, as this will go directly to the DPO.
- 2.2 The request will be managed by the DPO. You will be contacted for clarity about the information you want to see. Other people, such as tutors, Pastoral Managers, Child Protection Managers and potentially, the Principal may also be involved.
- 2.3 You will either be given the information you have asked for, or refused it, with an explanation of the reason. A common reason includes that the data is not retained/no longer retained.

#### **3 PROCEDURAL DETAILS**

- 3.1 Please click on this link: <https://forms.office.com/r/d0i4S3hyT3> and complete the online form or print the form in COMDA-A03-1-Data Protection- Subject Access Request or scan on the QR code presented on that form and complete the online process.
- 3.2 When you submit the form, your request has been sent to the Data Protection Officer. You will be given the opportunity to print off the form if you wish.

#### **4 PROCEDURE AUTHOR**

- 4.1 The author of this procedure is the Compliance Officer. They should be contacted for any points of clarification or suggested future amendments.



**PROCEDURE**

**5 VERSION CONTROL**

<b>Procedure Number</b>	COMDA-P03-1
<b>Procedure Name</b>	Freedom of Information –Subject Access Request
<b>Version Number</b>	00
<b>Publication Method</b>	External  A copy must be kept in U:\Staff Information\Policies\Procedures for Policies\COMmunications and DAta Procedures
<b>Approved by</b>	Full Trust Board
<b>Date of Approval</b>	February 2024
<b>Key changes since previous version</b>	This is a new procedure
<b>Next Review Date</b>	February 2025



**APPENDIX**

When complete please deliver to the Data Protection Officer at Heart of England School. This can be by email to [dataprotection@heart-england.co.uk](mailto:dataprotection@heart-england.co.uk) or by delivering to the Data Protection Officer at the school.

You can also complete the form <https://forms.office.com/r/d0i4S3hyT3> or scan this QR code:



- Please use this if you want to see the personal data of someone who previously or currently attends the school.
- You may be asked to verify your identity before personal data is provided to you.
- Anyone aged 16 and over can request to see their own data and must be involved when a Subject Access Request is made on their behalf.

<b>A. INFORMATION ABOUT THE REQUESTOR</b>									
<b>1. What is your name?</b> Block capitals									
<b>2. What is your email address?</b>									
<b>3. What is your phone number?</b>									
<b>4. What relationship do you have to the person whose data you are requesting?</b>	<table border="1"> <tbody> <tr> <td>I am a student at the school</td> <td></td> </tr> <tr> <td>I am the parent/carer of a student (aged under 16)</td> <td></td> </tr> <tr> <td>I am the parent/carer of a student (aged over 16)</td> <td></td> </tr> <tr> <td>Other (please complete "Status" question on next page).</td> <td></td> </tr> </tbody> </table>	I am a student at the school		I am the parent/carer of a student (aged under 16)		I am the parent/carer of a student (aged over 16)		Other (please complete "Status" question on next page).	
I am a student at the school									
I am the parent/carer of a student (aged under 16)									
I am the parent/carer of a student (aged over 16)									
Other (please complete "Status" question on next page).									



**APPENDIX**

<b>B. INFORMATION ABOUT THE PERSON WHOSE DATA IS BEING REQUESTED</b>													
<b>5. Full Legal Name of the person whose data being requested.</b> Block Capitals													
<b>C. CURRENT STUDENTS ONLY</b>													
<b>6. What year are they in?</b>	<table border="1"><tbody><tr><td>Year 7</td><td></td></tr><tr><td>Year 8</td><td></td></tr><tr><td>Year 9</td><td></td></tr><tr><td>Year 10</td><td></td></tr><tr><td>Year 11</td><td></td></tr><tr><td>Sixth Form</td><td></td></tr></tbody></table>	Year 7		Year 8		Year 9		Year 10		Year 11		Sixth Form	
Year 7													
Year 8													
Year 9													
Year 10													
Year 11													
Sixth Form													
<b>7. Who is their form tutor?</b>													
<b>D. STATUS</b>													
<b>8. Please give information on your status</b> (this only applies if not a current student at the school).	<table border="1"><tbody><tr><td>I am a current member of staff</td><td></td></tr><tr><td>I am a former member of staff</td><td></td></tr><tr><td>I am a former student</td><td></td></tr><tr><td>Other (please explain below)</td><td></td></tr><tr><td colspan="2"></td></tr></tbody></table>	I am a current member of staff		I am a former member of staff		I am a former student		Other (please explain below)					
I am a current member of staff													
I am a former member of staff													
I am a former student													
Other (please explain below)													
<b>E. SIGNATURE &amp; DATE SUBMITTED</b>													
<b>Signature</b>													
<b>Date</b>													

**APPENDIX**

**COMDA-A03-02-DATA PROTECTION – REPORT A DATA BREACH**

**1 INTRODUCTION**

1.1 The appendix holds the form to be used when reporting a data breach.

**2 DETAILS**

Complete the form on the next page and email it to [dataprotection@heart-england.co.uk](mailto:dataprotection@heart-england.co.uk)

**3 APPENDIX AUTHOR**

3.1 The author of this appendix is the Data Protection Officer. They should be contacted for any points of clarification or suggested future amendments.

**4 VERSION CONTROL**

<b>Appendix Number</b>	COMDA-A03-02
<b>Appendix Name</b>	Data Protection – Report a Data Breach
<b>Version Number</b>	00
<b>Publication Method</b>	External
<b>Approved by</b>	Full Trust Board
<b>Date of Approval</b>	July 2023
<b>Key changes since previous version</b>	1. This is a new appendix
<b>Next Review Date</b>	February 2024





**APPENDIX**

This must be completed within 24 hours of finding a data breach.  
It must then be emailed to [dataprotection@heart-england.co.uk](mailto:dataprotection@heart-england.co.uk)

<b>Data Breach number</b>	<b>DB0</b>							
<b>1. GENERAL INFORMATION</b>								
<b>Name and role of person reporting the data breach incident</b>								
<b>Date incident happened</b>								
<b>Date incident reported to DPO</b>								
<b>Method of reporting to DPO</b>	<table border="1"> <tr> <td>Verbal</td> <td></td> </tr> <tr> <td>Electronic</td> <td></td> </tr> <tr> <td>Paper</td> <td></td> </tr> </table>		Verbal		Electronic		Paper	
Verbal								
Electronic								
Paper								
<b>Date started to complete this form</b>								
<b><u>Description of incident</u></b> <i>If you 'caused' the breach please give plenty of detail here, the process you used, the time of day, your state of mind, what was happening around you etc.</i>								
<b><u>Purpose of this assessment</u></b>								
<p>The purpose of this assessment is to:</p> <ol style="list-style-type: none"> <li>1. Provide a consistent approach to categorising information security incidents.</li> <li>2. Determine whether the Information Commissioners Office should be notified about the incident.</li> <li>3. Provide an overview of the incident for the Principal / Chair of Governors along with recommendations on what action should be taken to address matters and to prevent a reoccurrence.</li> </ol> <p>Although there is no legal requirement on the School to report Information Security incidents which result in the loss, release or corruption of personal information, the Information Commissioner believes serious breaches should be brought to the attention of his office (ICO). The nature of the incident or loss can then be considered by the ICO, together with whether the School is properly meeting its responsibilities under the Data Protection Act.</p> <p>Serious breaches are not defined. Therefore, using the Information Commissioners own guidance entitled "<i>Notification of data security breaches to the Information Commissioners Office (ICO) – Ver 1 23 July 2012</i>" and the Department of Health guidance entitled "<i>Checklist for Reporting, managing and Investigating Information Governance Serious Untoward Incidents Gateway Ref: 13177 January 2010</i>", Solihull Council officers have developed this guidance for internal use in determining the Impact of a particular breach.</p> <p>This assessment will consider the:</p> <ul style="list-style-type: none"> <li>• Sensitivity of the information</li> <li>• Volume of information</li> <li>• Potential Detriment to Individuals</li> </ul>								



**APPENDIX**

2. DETAILS			
<b>How was the incident discovered</b>			
<b>Date incident discovered</b>			
<b>Type of incident (mark all that apply)</b>	Lost		Altered
	Stolen		Disclosed/wrongly made available
	Destroyed		Inadvertently copied
<b>How many data subjects could be affected (please provide estimate per category)?</b> <i>This must be a number, not e.g., "most of Y8" or "Y"</i>	Students		Trustees/Governors
	Adult Learners		Customers
	Alumni		Suppliers
	Parents/ Carers		General Public
	Employees		Other (specify below)
<b>Risk posed: categories of personal data included in the incident (mark all that apply).</b>	Data revealing racial or ethnic origin		
	Religious or philosophical beliefs		
	Sexual orientation data		
	Gender reassignment data		
	Health data		
	Basic personal identifiers e.g., name, contact details		
	Identification data e.g., usernames, passwords		
	Economic and financial data e.g., bank details credit card numbers		
	Official documents e.g., driving licences		
	Location data		
	Genetic or biometric data		
	Criminal convictions, offences		
	Not yet known		
	Other (give details below)		



**APPENDIX**

<b>3. CONTAINMENT</b>					
<b>Actions already taken.</b> <i>Summarise the actions taken to recover from the mistake and to stop it getting worse e.g., collected information, asked recipient to delete etc.)</i>					
<b>4. NOTIFICATION</b>					
<b>Who needs to know.</b> <b>Why they need to know.</b> <i>If there is anyone who needs to be informed, then list them below with your justification. It can be really important to let people know so that they can manage the consequences (against ID theft, fraud), however notification could also cause unnecessary worry. Also consider if there are any external organisations or regulatory bodies who need to be informed:</i>	<table border="1"><thead><tr><th>Who</th><th>Why</th></tr></thead><tbody><tr><td></td><td></td></tr></tbody></table>	Who	Why		
	Who	Why			
<b>5. CONFIRMATION</b>					
<b>Digital signature</b> <i>You do not need to print this form. To save paper and energy, please put your name here.</i>					
<b>Date completed form emailed to DPO</b>					

**APPENDIX**

**COMDA-A03-03-DATA PROTECTION – REVIEW A DATA BREACH**

**1 INTRODUCTION**

1.1 The appendix holds the form to be used when reviewing a reported data breach.

**2 DETAILS**

It must be completed by the Data Protection Officer (DPO) or a member of SLT if the DPO is not available/has caused the breach.

**3 APPENDIX AUTHOR**

3.1 The author of this appendix is the Data Protection Officer. They should be contacted for any points of clarification or suggested future amendments.

**4 VERSION CONTROL**

<b>Appendix Number</b>	COMDA-A03-03
<b>Appendix Name</b>	Data Protection – Review a Data Breach
<b>Version Number</b>	00
<b>Publication Method</b>	External
<b>Approved by</b>	Full Trust Board
<b>Date of Approval</b>	July 2023
<b>Key changes since previous version</b>	1. This is a new appendix
<b>Next Review Date</b>	February 2024

## APPENDIX

This must be completed as soon as possible after receiving a report of a data breach.

The time to complete does depend on the information given and the amount of investigation required. If the breach is to be reported to the ICO, it must be reported within 72 hours of its discovery.

Data Breach Number	DB0				
1. ASSESSMENT OF IMPACT					
Risk assessment models commonly categorise incidents according to the likely consequence, with the most serious being categorized as 5. Using the Department of Health and Information Commissioners guidance the following matrix is used to assess the impact of the incident.					
	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
<b>Sensitivity</b>	Minor breach of confidentiality but contained to single recipient. No sensitive personal data Breach contained and data retrieved within 2 hours.	As (1) but strong possibility that recipient has disclosed to others.	Unauthorised disclosure of limited personal data.  Some sensitive personal data involved.	As (3) but strong possibility that recipient has disclosed to others.	Unauthorised disclosure of particularly sensitive data e.g., health records or substantial personal data.
<b>Volume</b>	Up to 5 people affected.	Between 6 – 20 people affected or A single individual with a high volume of personal data	Between 21 and 100 people affected or Less than 20 people with a high volume of sensitive personal data.	Between 101-1000 people affected or Between 21 and 100 people with a high volume of sensitive personal data	Over 1000 people affected or Between 101-1000 people with a high volume of sensitive personal data
<b>Likelihood of Detriment</b>	No obvious detrimental effect on any individual.	Minor inconvenience for the individual. Potential for individual complaint.	Possibility for limited short-term distress Short term local media attention. Possibility of limited financial damage. Limited short-term embarrassment.	Limited longer-term distress Sustained local media coverage. Possibility for ID theft or fraud.	A real risk of serious harm or substantial longer-term distress. National media coverage. Strong possibility for ID theft, fraud and/or substantial financial damage.  Highly embarrassing.



**APPENDIX**

2. SUMMARY OF SCORE													
<table border="1"> <tr> <td>Sensitivity</td> <td></td> </tr> <tr> <td>Volume</td> <td></td> </tr> <tr> <td>Likelihood of detriment</td> <td></td> </tr> <tr> <td>TOTAL</td> <td></td> </tr> </table>	Sensitivity		Volume		Likelihood of detriment		TOTAL		<p><i>e.g., Sensitivity=3 (more than 1 person involved, but limited personal data disclosed), Volume = 2 (12 people affected), Likelihood of detriment=1 (nothing of significance is likely to happen)</i>  <i>Total=2+3+1=6</i></p> <p>A total over 10 more <b>must be</b> reported to the ICO.</p>				
Sensitivity													
Volume													
Likelihood of detriment													
TOTAL													
<b>To be reported to ICO?</b>	Y/N												
3. ACTION PLAN													
<p><b>Action required/Completed</b>  <i>Actions required to fix the problem, to mitigate any adverse effects (e.g., confirmed data sent in error has been destroyed, updated passwords, training planned) and when they took place.</i></p>													
<table border="1"> <thead> <tr> <th>Action required</th> <th>Date Completed</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Action required	Date Completed											
Action required	Date Completed												
<p><b>Communications Required/Completed</b>  <i>Names of people who have been informed and when (e.g. data subjects, other organisations (e.g. police/ LA/ ESFA/ DfE/ICO))</i></p>													
<table border="1"> <thead> <tr> <th>Communication required</th> <th>Date Completed</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Communication required	Date Completed											
Communication required	Date Completed												
<p><b>Reports to the ICO</b>  <i>If the incident has been reported to the ICO, give details of the ICO contact and attach any records/reports sent to them</i></p>													
<table border="1"> <thead> <tr> <th>Details of the ICO contact</th> <th>Date Completed</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <th>Reports send (include folder locations/file names)</th> <th>Date Completed</th> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Details of the ICO contact	Date Completed					Reports send (include folder locations/file names)	Date Completed					
Details of the ICO contact	Date Completed												
Reports send (include folder locations/file names)	Date Completed												
<p><b>I confirm that the details of this breach are accurate in accordance with the information known.</b></p>													
<b>Name of DPO</b>	Joan Fuller												
<b>Signed</b>													
<b>Date completed</b>													



**APPENDIX**

<b>4. PRINCIPAL/CHAIR OF GOVERNORS DECISION/RECOMMENDATION/SIGN OFF</b>	
The Principal/Chair of Governors have the report and investigation of this data breach and discussed the matters with relevant members of staff to reach the following conclusions:	
<ol style="list-style-type: none"><li>1. The incident is scored as ____ on the impact matrix (page 4) and is/is not reportable to the Information Commissioner.</li><li>2. [Add additional points as required]</li></ol>	
<b>Role of Signatory</b>	
<b>Signed</b>	
<b>Date completed</b>	