

# **Newham Community Learning - Data Protection Policy**

Last updated: September 2022

Applies to: Newham Community Learning

Approved by: Trust Board, September 2022



[newhamcommunitylearning.org](https://newhamcommunitylearning.org)

Tel: 0203 102 4002 | Email: [ceo.pa@newhamcommunitylearning.org](mailto:ceo.pa@newhamcommunitylearning.org) | [@NCLTrust](https://twitter.com/NCLTrust)  
Newham Community Learning, Sarah Bonnell School, Deanery Road, London E15 4LP

Newham Community Learning is a charitable company limited by guarantee and registered in England and Wales with Company Number 09896221. The registered office of the Trust is Sarah Bonnell School, Deanery Road, London, E15 4LP.

## Contents

<b>1. Overview of the Policy Management Process</b>	<b>4</b>
1.1. Document history	4
1.2. Review and approval	4
<b>2. Newham Community Learning - Data Protection Policy</b>	<b>5</b>
2.1. Introduction and purpose	5
2.2. Personal Data	5
2.3. The data protection principles	6
2.4. Conditions for processing in the first data protection principle	7
2.5. Use of personal data by Newham Community Learning	8
2.5.1. Pupils	8
2.5.2. Staff	8
2.5.3. Other individuals	9
2.6. Security of personal data	9
2.7. Disclosure of personal data to third parties	10
2.8. Data Protection Impact Assessments	11
2.9. Data processing arrangements	11
2.10. New Collection or use of personal data	11
2.11. Confidentiality of pupil concerns	12
2.12. Subject Access Requests	12
2.12.1. Exemptions to access by data subjects	13
2.13. Other rights of individuals	13
2.13.1. Right to object to processing	14
2.13.2. Right to rectification	14



2.13.3. Right to erasure	15
2.13.4. Right to restrict processing	15
2.13.5. Right to portability	16
2.13.6. Withdrawing consent	16
2.14. Breach of any requirement of the UK GDPR/Data Protection Act 2018	16
2.14.1. Notifying other parties	18
2.14.2. Preventing Future Breaches	18
2.14.3. Reporting internally after a breach	18
2.15. Contact	19



## 1. Overview of the Policy Management Process

### 1.1. Document history

Date	Revision	Version number (substantive revisions are allocated a new whole number; minor revisions are designated by the addition of a consecutive decimal point)
Sept 2021	Leading Learning Trust data protection policies in place; at NCST, school level policies in place regarding data protection  Leading Learning Trust Data Protection Policy reviewed by an external expert in September 2021	v1.0
Sept 2022	Leading Learning Trust Policy reviewed, updated and released as a Newham Community Learning Policy  Reflects the position of the COO as the Data Protection Officer at the Trust  Mechanics of how data protection works at all Trust schools forms part of the work of the IT, Cyber Security and Data Protection Working Group	v.2.0

### 1.2. Review and approval

The Data Protection Policy applies to the whole Trust. It is reviewed by the Executive Team (and/or their delegates) and is then presented to the Trust Board for approval (via a relevant board committee if appropriate).

It is reviewed in line with the Trust Policy Review Schedule.



## 2. Newham Community Learning - Data Protection Policy

This policy covers the key areas of data protection across the Trust. In areas of data protection, individual Trust schools have local arrangements in place/more detailed arrangements in place locally.

### 2.1. Introduction and purpose

Newham Community Learning collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with Newham Community Learning in order to provide education and associated functions. Newham Community Learning may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the UK General Data Protection Regulations, the Data Protection Act 2018, and other related legislation.

The UK GDPR applies to all personal data, held on our computer systems or in physical form in a filing system. It may also apply in a restricted way to manual unstructured data (which is data which is not held on our computer system and is not in a filing system).

This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and shall be reviewed annually.

Please note that this policy refers to the collection, storage and retention of personal data only; it does not apply to the preparation, storage or retention of teaching materials or any other materials used across the Trust or at our schools.

### 2.2. Personal Data

'Personal data' is any information about or related to an identified or identifiable individual. A *subset of personal data* is known as '*special category personal data*'. This special category data is information that relates to:

- race or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- physical or mental health;
- an individual's sex life or sexual orientation;



- genetic data, or biometric data for the purpose of uniquely identifying a natural person.

'Special category data' is given special protection, and additional safeguards apply if this information is processed in any way (including collection and usage).

Information relating to criminal convictions and offences shall only be held and processed where there is a lawful basis to do so.

Newham Community Learning does not intend to seek or hold special category personal data about staff or students except where Newham Community Learning has been notified of the information, or it comes to Newham Community Learning's attention via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice or as otherwise detailed in this policy. Staff or students are under no obligation to disclose to Newham Community Learning their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements). However, in instances where we are able to satisfy a condition of processing under Article 9 of GDPR (as well as a lawful basis for processing under Article 6), we do process these 'special categories' of data.

### 2.3. The data protection principles

The six data protection principles as laid down in the UK GDPR are followed at all times:

- personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;
- personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;
- personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;
- personal data shall be accurate and, where necessary, kept up to date;
- personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes;
- personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

In addition to this, Newham Community Learning is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail in paragraphs 7 and 8 below).



Newham Community Learning is committed to complying with the Data Protection Principles outlined below at all times. This means that Newham Community Learning will:

- inform individuals as to the purpose of collecting any information from them, as and when we ask for it (i.e. we ensure that at the point of collection, all data subjects are provided with a copy of our Privacy Notice, which details why we are collecting the data, how we store it, and how long we retain it for);
- be responsible for checking the quality and accuracy of the information;
- regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with our *Records Retention Policies* (available as separate policies held at school level);
- ensure that when information is authorised for disposal it is done appropriately;
- ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;
- share personal information with others only when it is necessary and legally appropriate to do so;
- set out clear procedures for responding to requests for access to personal information known as *Subject Access Requests* (outlined as part of this policy); and other requests from individuals seeking to use their individual rights; and
- report any breaches of the GDPR in accordance with the procedure as per the Breach Reporting outlined below.

## 2.4. Conditions for processing in the first data protection principle

Before any processing of personal data can occur, it is necessary to identify a legal basis under which to process that personal data. There are five possible legal bases available to Leading Learning Trust of processing and one must be identified for each processing task. The following are the five possible bases of processing (note that conditions for processing under Article 9 also need to be met where the processing is of 'special category' personal data):

- The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given.
- The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request.
- The processing is necessary for the performance of a legal obligation to which we are subject.
- The processing is necessary to protect the vital interests of the individual or another.



- The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us.

## 2.5. Use of personal data by Newham Community Learning

Newham Community Learning holds personal data on pupils, staff and other individuals such as visitors. In each case, the personal data must be treated in accordance with the data protection principles as outlined above.

### 2.5.1. Pupils

The personal data held regarding pupils includes contact details, assessment / examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.

The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well Newham Community Learning as a whole is doing, together with any other uses normally associated with this provision in a school environment.

Newham Community Learning may make use of limited personal data (such as contact details) relating to pupils, and their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with pupils of Newham Community Learning, but only where consent has been provided to this. In particular, Newham Community Learning may:

- make personal data, including special categories of personal data, available to staff for planning curricular or extra-curricular activities;
- use photographs of pupils in accordance with the *Photography Policies* that our schools have in place and the expression of parental preferences described therein, as well as consent collected via school systems.

Any wish to limit or object to any use of personal data should be notified to the Data Protection Officer - the Trust's COO - in writing. If, in the view of the DPO, the objection cannot be maintained, the individual will be given written reasons why Newham Community Learning cannot comply with their request.

### 2.5.2. Staff

The personal data held about staff will include contact details, employment history, information relating to career progression, information relating to DBS checks and photographs. Our *Records Retention Policies* held at school level detail how long this data is retained for.



The data is used to comply with legal obligations placed on Newham Community Learning in relation to employment, and the education of children in a school environment. Newham Community Learning may pass information to other regulatory authorities where appropriate, and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.

Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as “spent” once the period of the sanction has expired, the details of the incident may need to be kept for a longer period. All such records are maintained by Newham Partnership Working (npw) in their role as Data Processor, under the terms of the Human Resources Support and Payroll Support which they provide to Newham Community Learning. Contractual details specifying the role of npw as the Data Processor are in place and the roles and responsibilities are outlined. Staff records held at Trust schools are disposed of 6 years after the member of staff has left the employment of Newham Community Learning (as per our school *Records Retention Policies*).

Any wish to limit or object to any use of personal data should be notified to the Data Protection Officer (DPO) in writing, which notice will be acknowledged by the school concerned in writing. If, in the view of the school’s DPO, the objection cannot be maintained, the individual will be given written reasons why Newham Community Learning cannot comply with their request.

### 2.5.3. Other individuals

Newham Community Learning may hold personal information in relation to other individuals who have contact with the school, such as volunteers and guests. Such information shall be held only in accordance with the data protection principles, and shall not be kept longer than necessary and in line with the provisions in our *Records Retention Policies* held at school level.

## 2.6. Security of personal data

Newham Community Learning will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties.

All staff will be made aware of this Policy, and all associated policies, and their duties under the UK GDPR.

The Trust will take all reasonable and proportionate steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

## 2.7. Disclosure of personal data to third parties

The following list includes the most usual reasons that Newham Community Learning will authorise disclosure of personal data to a third party:



- to give a confidential reference relating to a current or former employee, volunteer or pupil;
- for the prevention or detection of crime;
- for the assessment of any tax or duty;
- where it is necessary to exercise a right or obligation conferred or imposed by law upon Newham Community Learning (other than an obligation imposed by contract);
- for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
- for the purpose of obtaining legal advice;
- for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);
- to publish the results of public examinations or other achievements of pupils of Newham Community Learning;
- to disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;
- to provide information to another educational establishment to which a pupil is transferring;
- to provide information to the Examination Authority as part of the examination process; and
- to provide information to the relevant Government Department concerned with national education. At the time of the writing of this Policy, the Government Department concerned with national education is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

The DfE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.

Newham Community Learning may receive requests from third parties (i.e. those other than the data subject, Newham Community Learning, and employees of Newham Community Learning) to disclose personal data it holds about pupils, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies.

Before sharing any personal data, consideration must be given to the potential need to carry out a Data Protection Impact Assessment.

Personal data must not be shared routinely unless the sharing is covered by existing documented data sharing arrangements. When relying on such an arrangement care should be taken to make sure that the sharing is within the agreed terms i.e. it is personal data of the sort covered by the arrangement and it is being shared for the purpose set out in the arrangement. If there is no



documented sharing agreement in place or the sharing does not appear to be covered by the existing arrangement then the DPO must be consulted. It is important that a data sharing decision is carefully considered and documented, even if it is a disclosure which will only be required very rarely.

All requests for the disclosure of personal data must be sent to the school's School Business Manager/local delegated senior member of staff, who will liaise with the Trust's Data Protection Officer (the COO) who will review and advise on whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure and ensuring that reasonable steps are taken to make sure that Newham Community Learning is being responsible in disclosing personal data, including checking that a third party organisation to whom personal data are to be disclosed meets a good standard of data protection compliance.

## 2.8. Data Protection Impact Assessments

Before any personal data is shared, the potential need for a Data Protection Impact Assessment (DPIA) to be carried out will be assessed having regard to the ICO guidance and checklists.

[Data protection impact assessments | ICO](#)

A DPIA must be carried out in any case where there is a high risk to individuals. In a case where high risk cannot immediately be ruled out a DPIA should be carried out as this is the best way to assess the level of risk.

## 2.9. Data processing arrangements

The Trust uses a number of data processors. A data processor processes personal data on the instructions of Newham Community Learning. Where an individual's personal data is processed by a data processor this is explained to them in the privacy notice provided to them. There must be a written data processing agreement in place for every data processing arrangement and no processor must be engaged without such an agreement being in place. If a member of staff wishes to use a new processor then the DPO must be consulted as a full due diligence process will need to be carried out before any personal data is disclosed to the processor.

## 2.10. New Collection or use of personal data

If a member of staff intends to collect additional personal data or deploy existing personal data for a new purpose, then they must consult the DPO. A data protection impact assessment may need to be carried out and there may be a need to update documentation such as the central record of processing activities and privacy notices.

## 2.11. Confidentiality of pupil concerns



Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, Newham Community Learning will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, *or* where Newham Community Learning believes disclosure will be in the best interests of the pupil or other pupils.

Details of how this process is managed are provided in our Child Protection and Safeguarding Policy, which is available on our Trust website.

## 2.12. Subject Access Requests

Anybody who makes a request to see any personal information held about them by Newham Community Learning is making a subject access request. All information relating to the individual which is held in electronic form or in a manual filing system should be considered for disclosure.

Further to the receipt of either a verbal or a written request, the requester will be asked to complete the Trust Subject Access Request Form and bring it into the School Office. As noted on the form, the requester will be required to present suitable forms of identification to school office staff, in person, before the subject access request can be actioned. Once office staff are satisfied with the proof of identity presented, the request will be actioned. It will be passed to the Data Protection Officer (DPO) - and as per the GDPR, a response will be provided within one month except where the period for a response may be extended by up to a further two months because of the complexity or number of requests. Where an extension is necessary, the individual will be informed of it within one month of receipt of the request, together with the reasons for the delay. Please note that as per the Policy, responses will be provided in electronic format, unless requested otherwise.

Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The DPO must, however, be satisfied that:

- the child or young person lacks sufficient understanding; and
- the request made on behalf of the child or young person is in their interests.

Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances Newham Community Learning must have written evidence that the individual has authorised the person to make the application and the DPO must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.



Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence.

An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

All files must be reviewed by the DPO before any disclosure takes place. Access will not be granted before this review has taken place, although the one month time limit on disclosure (or reporting why a disclosure cannot be made) must always be respected unless the deadline has been extended as detailed above.

Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

### **2.12.1. Exemptions to access by data subjects**

Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

There are other exemptions from the right of subject access. If we intend to apply any of them to a request then we will usually explain which exemption is being applied and why.

## **2.13. Other rights of individuals**

Newham Community Learning has an obligation to comply with the rights of individuals under the law, and takes these rights seriously. The following section sets out how Newham Community Learning will comply with the rights to:

- object to processing;
- rectification;
- erasure; and
- data portability.

There is no charge for individual rights requests except where the requests are manifestly unfounded or excessive in which case Leading Learning Trust may either:

- (a) charge a reasonable fee to cover administrative costs, or



(b) Refuse to act on the request(s).

### **2.13.1. Right to object to processing**

An individual sometimes has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest where they do not believe that those grounds are made out.

Where such an objection is made, it must be sent to the DPO at the school concerned. Within 2 working days of receipt by the school, the DPO will assess whether there are compelling grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings or one of the other allowable exceptions.

The DPO shall be responsible for notifying the individual of the outcome of their assessment without undue delay and within one month (of receipt of satisfactory identification documents). This deadline may be extended by up to a further two months because of the complexity or number of requests. Where an extension is necessary, the individual will be informed of it within one month of receipt of the request, together with the reasons for the delay.

### **2.13.2. Right to rectification**

An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to the DPO of the school concerned within 2 working days of receipt by the school, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall be given the option of lodging a complaint as per the Complaints Policy (available on the Trust website) or an appeal direct to the Information Commissioner.

An individual also has a right to have incomplete information completed by providing the missing data; any information submitted in this way shall be updated without undue delay and within one month except where the period for a response may be extended by up to a further two months because of the complexity or number of requests. Where an extension is necessary, the individual will be informed of it within one month of receipt of the request, together with the reasons for the delay.

Where the personal data has been disclosed to another party, that party will be informed of the rectification unless this proves impossible or involves disproportionate effort.



### 2.13.3. Right to erasure

Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

- where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;
- where consent is withdrawn and there is no other legal basis for the processing;
- where an objection has been raised under the right to object, and found to be legitimate;
- where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met); and
- where there is a legal obligation on Newham Community Learning to delete.

The DPO will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other Data Controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

A response will be given without undue delay and within one month except where the period for a response may be extended by up to a further two months because of the complexity or number of requests. Where an extension is necessary, the individual will be informed of it within one month of receipt of the request, together with the reasons for the delay.

### 2.13.4. Right to restrict processing

In the following circumstances, processing of an individual's personal data may be restricted:

- where the accuracy of data has been contested, during the period when Newham Community Learning is attempting to verify the accuracy of the data;
- where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;
- where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim; and/or
- where there has been an objection made, pending the outcome of any decision.

A response will be given without undue delay and within one month except where the period for a response may be extended by up to a further two months because of the complexity or number of requests. Where an extension is necessary, the individual will be informed of it within one month of receipt of the request, together with the reasons for the delay.



The DPO at the school concerned will make a decision regarding any application for the restriction of personal data. Where a decision is made to restrict the data, the individual must be informed before the restriction is lifted.

#### **2.13.5. Right to portability**

If an individual wants to send their personal data to another organisation they have a right to request that Newham Community Learning provides their information in a structured, commonly used, and machine readable format. As this right is *limited to situations where Newham Community Learning is processing the information on the basis of consent or performance of a contract and the personal data was provided by the individual*, the situations in which this right can be exercised will be quite limited. If a request for this is made, it should be forwarded to the school-based DPO within 2 working days of receipt by the school, and they will review and revert as necessary.

A response will be given without undue delay and within one month except where the period for a response may be extended by up to a further two months because of the complexity or number of requests. Where an extension is necessary, the individual will be informed of it within one month of receipt of the request, together with the reasons for the delay.

#### **2.13.6. Withdrawing consent**

If an individual wants to withdraw their consent, they may do so at any time but the withdrawal of consent will not affect the validity of anything done prior to the consent being withdrawn. If a request for this is made, it should be forwarded to the school-based DPO within 2 working days of receipt by the school, and they will review and revert as necessary.

### **2.14. Breach of any requirement of the UK GDPR/Data Protection Act 2018**

Any and all breaches or suspected breaches of the UK GDPR, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to the Data Protection Officer (DPO).

The Headteacher shall immediately lead an investigation into what has happened and take measures to contain the breach, where containment is possible, delegating tasks to staff but retaining the coordinating role.

Once notified, the DPO shall assess and document whether the breach is one which meets the definition of 'Personal Data Breach': the definition is '*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 assessment shall include:



- the extent of the breach, including the amount of personal data and number of people affected;
- the type of personal data involved i.e how sensitive it is - and whether it contains special category information.
- the risks to the data subjects as a consequence of the breach;
- any security measures in place that will protect the information such as encryption, password protection, pseudonymisation;
- any measures that can be taken immediately to mitigate the risk to the individuals.

Where the definition of Personal Data Breach is met, unless the DPO concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of Newham Community Learning, unless a delay can be justified. The Information Commissioner shall be told:

- details of the breach, including the volume of data at risk, and the number and categories of data subjects;
- the contact point for any enquiries (which shall usually be the Data Protection Officer);
- the likely consequences of the breach; and
- measures proposed or already taken to address the breach.

If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then data subjects will be notified of the breach without undue delay unless the data would be unintelligible to those not authorised to access it (e.g. it is encrypted), or measures have been taken to mitigate any risk to the affected individuals such that the high risk is no longer likely to materialise. Note that breaches do not have to be notified to data subjects if the risk is not high or disproportionate effort would be required to provide such notification. In the case where individual notification would be disproportionate, there must be a public communication or similar measure whereby the affected individuals are informed in an equally effective manner.

Data subjects shall be told:

- the nature of the breach;
- who to contact with any questions;
- measures taken to mitigate any risks.
- Anything further which may allow them to protect themselves e.g. to watch out for phishing emails or to change passwords.

The Data Protection Officer (DPO) shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented and what measures should be taken from now on to prevent such a breach from happening in the future. Any



recommendations for further training or a change in procedure shall be reviewed by the trust board and a decision made about implementation of those recommendations.

A Personal Data breach will be logged by the DPO. The record must comprise the facts relating to the breach, its effects and remedial action taken.

#### **2.14.1. Notifying other parties**

The DPO shall consider and advise the relevant Headteacher on whether any other authorities or third parties (apart from the ICO and affected individuals) should be notified. This may include:

- The ESFA (as a Serious Incident Report in line with the Charity Commission Guidance or as required by The Academy Trust Handbook 2021 - Section entitled 'Fraud, Theft, Irregularity and Cyber Crime')
- Leading Learning Trust's insurer or the RPA (Risk Protection Arrangement for Academies)
- The Local Authority
- Parents of affected pupils
- The police (e.g. theft of equipment or data)
- Any other third parties

#### **2.14.2. Preventing Future Breaches**

Once the data breach has been dealt with, Newham Community Learning will consider its security measures, practices, policies and procedures in order to make any necessary improvements to prevent such a breach from happening again. This consideration could include the following, as examples:

- existing security measures and whether any further technical or organisational measures are required;
- existing staff awareness and whether there is a need for further staff briefings or further training;
- whether it is necessary to conduct or review data protection impact assessments (DPIAs);
- further audit; and/or
- policy and procedure reviews

#### **2.14.3. Reporting internally after a breach**

Any personal data breach or 'near miss' must be reported to the Trust Board and any relevant committees or working groups in place.

The Senior Leadership Team and staff should be debriefed as appropriate following the investigation.



## 2.15. Contact

If anyone has any concerns or questions in relation to this policy or wishes to exercise their individual data protection rights they should contact the Data Protection Officer (DPO).

Any queries regarding the Trust's data protection arrangements should be addressed to the CEO's PA, who can be contacted on [ceo.pa@newhamcommunitylearning.org](mailto:ceo.pa@newhamcommunitylearning.org).

