DATA PROTECTION POLICY

Document Owner: Data Protection Officer
Date: September 2020
Status: Statutory

Document Type		Data Protection Policy			
Reference Number		CLT-DPP-V3.0			
Summary		The City Learning Trust (the Trust) aims to ensure that all personal data collected by the Trust and our Academies, about staff, pupils/students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) .			
Associated Documents		Use Your Own Device (UYOD) Policy CCTV Policy Freedom of Information Policy Online Safety Policy Child Protection and Safeguarding Policy Remote Learning and Online Communication Acceptable Use Statement Retention Policy Privacy Notices			
Target Audience		All Employees			
Document Version No:		V3.0			
Date of this Version		September 2020			
Document Owner		Data Protection Officer			
Review Body		Policy & Procedures Working Party			
Union Consultation Date/s:		n/a			
Review Body Meeting Date					
Approved/Ratified by		Board of Trustees			
Approval Date		8th April 2019 14th December 2020			
Date uploaded on website/s					
CLT	Haywood	Trentham	Mill Hill	Smallthorne	
Review Frequency		Bi-annual			
Review Date:		April 2022			
Signature of Chair of Trustees					
Acknowledged by:	**Local Governing Committee:**				
	Haywood 10.7.19 24.3.20	Trentham 3.7.19 25.3.20	Mill Hill 26.6.18 19.6.19 18.3.20	Smallthorne 9.7.19 18.3.20	

VERSION CONTROL

Version No:	Type of change	Date	Revisions from previous version
V1	New Document		Policy written to be GDPR compliant
V2	Review for GDPR	Sept 2019	Policy reviewed and update to reflect the Data Protection Act 2018 and latest ICO guidance.
V3	Bi-annual review	May 2020	Policy reviewed and update with regard to blended learning.

TABLE OF CONTENTS

VERSION CONTROL 2
1. STATUS 5
2. AIMS 5
3. LEGISLATION AND GUIDANCE 5
4. DEFINITIONS 5
4.1 Personal Data 5
4.2 Special Categories of Personal Data 5
4.3 Processing 5
4.4 Data Subject 6
4.5 Data Controller 6
4.6 Data Processor 6
4.7 Personal Data Breach 6
5. THE DATA CONTROLLER 6
6. ROLES AND RESPONSIBILITIES 6
6.1 Board of Trustees 6
6.2 Data Protection Officer 6
6.3 Headteacher/Principal 6
6.4 All Staff 6
7. DATA PROTECTION PRINCIPLES 7
8. COLLECTING PERSONAL DATA 7
8.1 Lawfulness, Fairness and Transparency 7
8.2 Limitation, Minimisation and Accuracy 8
9. SHARING PERSONAL DATA 8
10. SUBJECT ACCESS REQUESTS & OTHER RIGHTS OF INDIVIDUALS 9
10.1 Subject Access Requests 9
10.2 Children and Subject Access Requests 9
10.2.1 Primary School Children: 9
10.2.2 Secondary School Children: 9
10.3 Responding to Subject Access Requests 9
10.4 Other Data Protection Rights of the Individual 10
11. BIOMETRIC RECOGNITION SYSTEMS 10
12. CCTV 11
13. PHOTOGRAPHS AND VIDEOS 11
13.1 Primary Academies 11
13.2 Secondary Academies 11
14. DATA PROTECTION BY DESIGN AND DEFAULT 11
15. DATA SECURITY AND STORAGE OF RECORDS 12
16. DISPOSAL OF RECORDS 12
17. PERSONAL DATA BREACHES 13
18. TRAINING 13
19. MONITORING AND REVIEW 13
20. LINKS WITH OTHER POLICIES 13

APPENDIX A 14
Personal Data Breach Procedure 14
Actions to Minimise the Impact of Data Breaches 15

1. STATUS

a. Statutory.

2. AIMS

a. The City Learning Trust (the Trust) aims to ensure that all personal data collected by the Trust and our Academies, about staff, pupils/students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Act 2018.

b. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

3. LEGISLATION AND GUIDANCE

a. This policy meets the requirements of the GDPR DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

b. It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

c. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

d. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

e. In addition, this policy complies with our funding agreement and articles of association.

f. This Policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation.

4. DEFINITIONS

4.1 Personal Data

a. Any information relating to an identified, or identifiable, living individual.

b. This may include the individual's:

   i. Name (including initials)
   ii. Identification number
   iii. Location data
   iv. Online identifier, such as a username

c. 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

a. Personal data which is more sensitive and so needs more protection, including information about an individual's:

   ii. Racial or ethnic origin
   iii. Political opinions
   iv. Religious or philosophical beliefs
   v. Trade union membership
   vi. Genetics
   vii. Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
   viii. Health – physical or mental
   ix. Sex life or sexual orientation

4.3 Processing

a. Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.

b. Processing can be automated or manual.

4.4 Data Subject

a. The identified or identifiable individual whose personal data is held or processed.

4.5 Data Controller

a. A person or organisation that determines the purposes and the means of processing of personal data.

4.6 Data Processor

a. A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

4.7 Personal Data Breach

a. A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

5. THE DATA CONTROLLER

a. The Trust and our Academies process personal data relating to parents, pupils/students, staff, governors, visitors and others, and therefore are data controllers.

b. The Trust is registered as a data controller with the ICO and has paid its data protection fee to the ICO as legally required.

6. ROLES AND RESPONSIBILITIES

a. This policy applies to **all staff** employed by the Trust, volunteers who work in member academies and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

6.1 Board of Trustees

The City Learning Trust Board of Trustees (the Board of Trustees) has overall responsibility for ensuring that the Trust and member Academies comply with all relevant data protection obligations.

6.2 Data Protection Officer

a. The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

b. The DPO will provide an annual report of their activities directly to the Board of Directors and, where relevant, report to the Board advice and recommendations on Trust data protection issues.

c. The DPO is also the first point of contact for individuals whose data the Trust and our Academies process, and for the ICO.

d. Full details of the DPO's responsibilities are set out in their job description.

e. Our DPO is Joanne Shaw and is contactable via City Learning Trust, High Lane Burslem, Stoke on Trent, ST6 7AB, Tel No: 07940514736 Email: jshaw@citylearningtrust.org

6.3 Headteacher/Principal

a. The Headteacher/Principal, in each member Academy, acts as the representative of the data controller, in their Academy, on a day-to-day basis.

6.4 All Staff

a. Staff are responsible for:

   i. Collecting, storing and processing any personal data in accordance with this policy
   ii. Informing the Academy of any changes to their personal data, such as a change of address
   iii. 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
- 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

7. DATA PROTECTION PRINCIPLES

a. The GDPR is based on data protection principles that the Trust and member Academies must comply with.

b. The principles say that personal data must be:

   i. Processed lawfully, fairly and in a transparent manner
   ii. Collected for specified, explicit and legitimate purposes
   iii. Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
   iv. Accurate and, where necessary, kept up to date
   v. Kept for no longer than is necessary for the purposes for which it is processed
   vi. Processed in a way that ensures it is appropriately secure

c. This policy sets out how the Trust aims to comply with these principles.

8. COLLECTING PERSONAL DATA

8.1 Lawfulness, Fairness and Transparency

a. We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

   i. The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
   ii. The data needs to be processed so that the school can comply with a legal obligation
   iii. The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
   iv. The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions
   v. The data needs to be processed for the legitimate interests of the school (where the processing is not for any tasks the school performs as a public authority) or a third party provided the individual's rights and freedoms are not overridden.
   vi. The individual (or their parent/carer when appropriate in the case of a pupils/students) has freely given clear consent

b. For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

   i. The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent
   ii. The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
   iii. The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
   iv. The data has already been made manifestly public by the individual
   v. The data needs to be processed for the establishment, exercise or defence of legal claims
   vi. The data needs to be processed for reasons of substantial public interest as defined in legislation
   vii. The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
   viii. The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
   ix. The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

c. For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:
    i. The individual (or their parent/carer when appropriate in the case of a pupil) has given consent
    ii. The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
    iii. The data has already been made manifestly public by the individual
    iv. The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
    v. The data needs to be processed for reasons of substantial public interest as defined in legislation

f. Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

g. We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

8.2 Limitation, Minimisation and Accuracy

a. We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

b. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

c. Staff must only process personal data where it is necessary in order to do their jobs.

d. We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

e. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymized. This will be done in accordance with The City Learning Trust's Retention Policy.

9. SHARING PERSONAL DATA

a. We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:
    i. There is an issue with a pupil/student or parent/carer that puts the safety of our staff at risk
    ii. We need to liaise with other agencies – we will seek consent as necessary before doing so.
    iii. Our suppliers or contractors need data to enable us to provide services to our staff and pupils/ students – for example, IT companies and online service providers for provision of remote learning and online communication practice. When doing this, we will:
        - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
        - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
        - Only share data that the supplier or contractor needs to carry out their service.

b. We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

c. We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils/students or staff.

d. Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

10. SUBJECT ACCESS REQUESTS & OTHER RIGHTS OF INDIVIDUALS

10.1 Subject Access Requests

a. Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:
   i. Confirmation that their personal data is being processed
   ii. Access to a copy of the data
   iii. The purposes of the data processing
   iv. The categories of personal data concerned
   v. Who the data has been, or will be, shared with
   vi. How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
   vii. Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing.
   viii. The right to lodge a complaint with the ICO or another supervisory authority.
   ix. The source of the data, if not the individual
   x. Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
   xi. The safeguards provided if the data is being transferred internationally.

b. Subject access requests must be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:
   iii. Name of individual
   iv. Correspondence address
   v. Contact number and email address
   vi. Details of the information requested

c. If staff receive a subject access request they must immediately forward it to the Academy Principal/ Headteacher who will inform the DPO.

10.2 Children and Subject Access Requests

a. Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

10.2.1 Primary School Children:

a. Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our Primary Academies may be granted without the express permission of the pupils. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

10.2.2 Secondary School Children:

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our Academies may not be granted without the express permission of the students. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

10.3 Responding to Subject Access Requests

a. When responding to requests, we:
   i. May ask the individual to provide 2 forms of identification.
   ii. May contact the individual via phone to confirm the request was made.
   iii. Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant).
   iv. Will provide the information free of charge.

v. May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

b. We will not disclose information for a variety of reasons, such as if it:

iii. Might cause serious harm to the physical or mental health of the pupils/students or another individual.
iv. Would reveal that the child is being abused or at risk of abuse, where the disclosure of that information would not be in the child's best interests.
v. Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it.
vi. Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam script.

c. If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

d. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

10.4 Other Data Protection Rights of the Individual

a. In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

i. Withdraw their consent to processing at any time
ii. Ask us to rectify, erase or restrict processing of their personal data, (in certain circumstances)
iii. Prevent use of their personal data for direct marketing
iv. Object to processing which has been justified on the basis of public interest, official authority or legitimate interest.
v. Challenge decisions based solely on automated decision making on profiling (ie making decisions or evaluating certain things about an individual based on their personal data with no human involvement).
vi. Be notified of a data breach in certain circumstances
vii. Make a complaint to the ICO
viii. Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

b. Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the Academy Principal/Headteacher who will inform the DPO.

11. BIOMETRIC RECOGNITION SYSTEMS

a. Where our Academies use pupils'/students' biometric data as part of an automated biometric recognition system (for example, pupils/students use finger prints to receive school dinners instead of paying with cash we will comply with the requirements of the Protection of Freedoms Act 2012. (NB that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18).

b. Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The Academies will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

c. Parents/carers and pupils/students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils/students. For example, pupils/students can pay for school dinners in cash at each transaction if they wish.

d. Parents/carers and pupils/students can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

e. As required by law, if a pupil/student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's/student's parent(s)/carer(s).

f. Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

a. We use CCTV in various locations around the academies' sites to ensure they remain safe. We will adhere to the ICO's code of practice for the use of CCTV.

b. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

c. Any enquiries about the CCTV system should be directed to the Data Protection Officer.

13. PHOTOGRAPHS AND VIDEOS

a. As part of our Academy activities, we may take photographs and record images of individuals within our Academies.

13.1 Primary Academies

a. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parents/carers and pupils.

13.2 Secondary Academies

a. We will obtain written consent from parents/carers, or pupils/students aged 13 and over, for photographs and videos to be taken of pupils/students for communication, marketing and promotional materials.

b. Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupils/students. Where we don't need parental consent, we will clearly explain to the pupils/students how the photograph and/or video will be used.

c. Uses may include:

   iv. Within school on notice boards and in school magazines, brochures, newsletters, etc.
   v. Outside of school by external agencies such as the school photographer, newspapers, campaigns
   vi. Online on our school website or social media pages

d. 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.

e. Any photographs and videos taken by parent/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other students/pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

14. DATA PROTECTION BY DESIGN AND DEFAULT

a. We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

   i. Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
   ii. Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
   iii. Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)

iv. Integrating data protection into internal documents including this policy, any related policies and privacy notices
v. Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
vi. Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
vii. Appropriate safeguards being put in place if we transfer any personal data outside the European Economic Area (EEA), where different data protection laws apply.
viii. Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure.

15. DATA SECURITY AND STORAGE OF RECORDS

a. We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

b. In particular:

i. Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
ii. Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
iii. Where personal information needs to be taken off site, staff must sign it in and out from the school office
iv. Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils/students are reminded to change their passwords at regular intervals
v. Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
vi. Staff, pupils/students or governors who store personal data on their personal devices are expected to follow the same security procedures as for school-owned equipment. See the CLT's UYOD Policy.
vii. Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

16. DISPOSAL OF RECORDS

a. We will effectively manage and audit data (both in physical and electronic format) by complying with the City Learning Trust's Records and Management Policy.

b. Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

c. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. PERSONAL DATA BREACHES

a. The school will make all reasonable endeavors to ensure that there are no personal data breaches.

b. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

c. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

   i. A non-anonymised dataset being published on the school website which shows the exam results of pupils/students eligible for the pupils' premium
   ii. Safeguarding information being made available to an unauthorised person
   iii. The theft of a school laptop containing non-encrypted personal data about pupils/students

18. TRAINING

a. All staff and governors are provided with data protection training as part of their induction process.

b. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. MONITORING AND REVIEW

a. The DPO is responsible for monitoring and reviewing this policy.

b. This policy will be reviewed **every 2 years** and shared with the Trust Board and Local Governing Bodies of our Academies

20. LINKS WITH OTHER POLICIES

a. This Data Protection Policy is related to Trust and Academy Policies & documents in the following areas:

   i. Use Your Own Device (UYOD) Policy
   ii. CCTV Policy
   iii. Freedom of Information Policy
   iv. Online Safety Policy
   v. Child Protection and Safeguarding Policy
   vi. Remote Learning and Online Communication Acceptable Use Statement
   vii. Retention Policy
   viii. Privacy Notices

APPENDIX A

Personal Data Breach Procedure

a. This procedure is based on guidance on personal data breaches produced by the ICO.

b. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO. A clear description of the breach must be provided.

c. The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
   i. Lost
   ii. Stolen
   iii. Destroyed
   iv. Altered
   v. Disclosed or made available where it should not have been
   vi. Made available to unauthorised people

d. The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

e. The DPO will alert the Headteacher/Principal and the Chair of the Board of Directors

f. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

g. The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
   i. Loss of control over their data
   ii. Discrimination
   iii. Identify theft or fraud
   iv. Financial loss
   v. Unauthorised reversal of pseudonymisation (for example, key-coding)
   vi. Damage to reputation
   vii. Loss of confidentiality
   viii. Any other significant economic or social disadvantage to the individual(s) concerned

h. If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

i. The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on a secured area on the computer network.

j. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website or through their breach report line (0303 123 1113), within 72 hours. As required, the DPO will set out:
   i. A description of the nature of the personal data breach including, where possible:
      - The categories and approximate number of individuals concerned
      - The categories and approximate number of personal data records concerned
   ii. The name and contact details of the DPO
   iii. A description of the likely consequences of the personal data breach
   iv. A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

k. If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

l. The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    i. The name and contact details of the DPO
    ii. A description of the likely consequences of the personal data breach
    iii. A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

g. The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

h. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    i. Facts and cause
    ii. Effects
    iii. Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

h. Records of all breaches will be stored on a secured area on the computer network.

i. The DPO and Headteacher/Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to Minimise the Impact of Data Breaches

a. We will take the actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.