

| | | |
|---|---------------------------|--|
|  | Name of School | Corbets Tey School |
| | Policy Review Date | 18th November 2020 |
| | Next Review Date | Summer 2021 |
| | Reviewed by | Governor Name: Julie Lamb Governor Signature:  |

Data Protection Policy

Introduction

Corbets Tey School recognises and accepts its responsibility as set out in the Data Protection Act 2018 and sub-legislation contained therein. The School, as a Data Controller, will take all reasonable steps to meet this responsibility and to promote good practice in the handling and use of personal information. In particular, the School will comply with the Data Protection Principles set out in the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

Equality Impact Assessment

The school aims to design and implement services, policies and procedures that meet the diverse needs of our provision, population and workforce, ensuring that none are placed at an unreasonable or unfair disadvantage over others. We are confident that this policy does not place anyone at an unreasonable or unfair disadvantage, and is compliant with relevant equalities legislation.

Scope

The School needs to collect and use certain types of personal information about people with whom it deals in order to operate. These include current, past and prospective employees, students, suppliers, clients, and others with whom it communicates. In addition, it may be required by law to collect and use certain types of information to comply with the requirements of government departments. This personal information must be dealt with properly however it is collected, recorded and used - whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this in the Data Protection Act 2018 and the General Data Protection Regulations, 25th May 2018.

We regard lawful and correct treatment of personal information by the School as very important, in order to secure the successful carrying out of operations and the delivery of our services, and to maintain confidence with those whom we deal. The School wishes to ensure that it treats personal information lawfully, correctly and in compliance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

Contents

| | |
|--|----|
| 1. Aims | 3 |
| 2. Legislation and guidance..... | 3 |
| 3. Definitions | 3 |
| 4. The data controller | 4 |
| 5. Roles and responsibilities..... | 4 |
| 6. Data protection principles..... | 5 |
| 7. Collecting personal data..... | 5 |
| 8. Sharing personal data | 7 |
| 9. Subject access requests and other rights of individuals | 7 |
| 10. Parental requests to see the educational record..... | 10 |
| 11. CCTV | 10 |
| 12. Photographs and videos | 10 |
| 13. Data protection by design and default..... | 11 |
| 14. Data security and storage of records | 11 |
| 15. Disposal of records | 12 |
| 16. Personal data breaches | 12 |
| 17. Training..... | 12 |
| 18. Monitoring arrangements | 12 |
| 19. Links with other policies | 12 |
| Appendix 1: Personal data breach procedure..... | 13 |
| Appendix 2: Job Description – Data Protection Officer (DPO)..... | 16 |

1. Aims

Our school aims to ensure that all personal data collected about staff, 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 Data Protection Act 2018 (DPA 2018).

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

2. Legislation and guidance

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

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

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.

3. Definitions

| TERM | DEFINITION |
|--|---|
| Personal data | <p>Any information relating to an identified, or identifiable, living individual. This may include the individual's:</p> <ul style="list-style-type: none"> • Name (including initials) • Identification number • Location data • Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p> |
| Special categories of personal data | <p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation |
| Processing | <p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.</p> |
| Data subject | <p>The identified or identifiable individual whose personal data is held or processed.</p> |
| Data controller | <p>A person or organisation that determines the purposes and the means of processing of personal data.</p> |

| TERM | DEFINITION |
|-----------------------------|---|
| Data processor | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. |
| Personal data breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. |

4. The data controller

Our school processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

The school has paid its data protection fee to the ICO, as legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and supporting the school SLT and Governors in developing related policies and guidelines where applicable. The DPO will also monitor that the procedures contained within this and related policies is communicated appropriately to school staff.

They will provide an annual report of their activities directly to the governing board at each Summer Term Full Governing Board Meeting and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description (Appendix 2).

Our DPO is Christine MacPherson and is contactable via dpo@corbetstey.havering.sch.uk

5.3 Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school 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
- 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. Data protection principles

The GDPR is based on data protection principles that our school must comply with. 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

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

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

- 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
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest** or exercise its official authority
- The data needs to be processed for the **legitimate interests** of the school or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent or carer when appropriate in the case of a student) has freely given clear **consent**

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

- The individual (or their parent or carer when appropriate in the case of a student) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- 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

- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- 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
- 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
- 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

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent or carer when appropriate in the case of a student) has given **consent**
- 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
- The data has already been made **manifestly public** by the individual
- 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**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

We will always consider the fairness of our data processing. We will ensure that 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.

7.2 Limitation, minimisation and accuracy

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.

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.

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

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

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's **Records Management Policy**.

8. Sharing personal data

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:

- There is an issue with a student, parent or carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
 - Only appoint suppliers or contractors who 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, and information necessary to keep them safe while working with us

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

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 students or staff.

Where we transfer personal data internationally, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form, they must immediately forward it to the DPO.

9.2 Children and subject access requests

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.

Children below the age of 12 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 students at our school may be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 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 school may not be granted without the express permission of the student. However, as many of our students have learning needs this may not be possible or purposeful and the necessity for obtaining a student's permission will be decided on a case by case basis, taking all relevant factors into account. Capacity decisions will be made by experienced key school staff who have undertaken training in the Mental Capacity Act. The DPO will be informed of all capacity decisions and these will all be recorded.

When deciding on the capacity of a child or an adult with a disability to give permission the principles of the Mental Capacity Act 2005 should be applied as follows:

The starting assumption should always be that the person has capacity. The Act details a two-stage test of capacity:

1. Does the person have an impairment, or a disturbance in the functioning, of their mind or brain?
2. Does the impairment or disturbance mean that the person is unable to make a specific decision when they need to? You should offer all appropriate and practical support to achieve this before applying this stage of the test.

Functional tests of capacity

To be able to make a decision a person should be able to:

- **Understand the decision to be made** and the information provided about the decision. The consequences of making a decision must be included in the information given.
- **Retain the information** – a person should be able to retain the information given for long enough to make the decision.
- **Use that information in making the decision** – a person should be able to weigh up the pros and cons of making the decision.
- **Communicate their decision** – if a person cannot communicate their decision. You should make all efforts to help the person communicate their decision before deciding they cannot.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm the requester's identity, where relevant)
- Will provide the information free of charge but a charge may be made for actual disbursements such as:
 - photocopying
 - postage and packaging

- the costs directly incurred as a result of viewing information

Please refer to the school's Freedom of Information Policy for further details.

- 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

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- 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
- 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 scripts

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

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.

9.4 Other data protection rights of the individual

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:

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

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 DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a student) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the student concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the student or another individual, or if it would mean releasing exam marks before they are officially announced.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

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.

Any enquiries about the CCTV system should be directed to – Karen Hoffman (Site Administrator)

12. Photographs and videos

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

We will obtain written consent from parents or carers, or students aged 18 and over (if appropriate - see section 9.2 regarding capacity assessments), for photographs and videos to be taken of students for communication, marketing and promotional materials.

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

Any photographs and videos taken by parents or 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 are not shared publicly on social media for safeguarding reasons, unless all the relevant parents or carers (or students where appropriate) have agreed to this.

Where the school takes photographs and videos, uses may include:

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

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.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our **Child Protection and Safeguarding Policy, Remote Learning Policy and Staff Photo Policy** for more information on our use of photographs and videos.

13. Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- 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)
- 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)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep records of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply
- 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

14. Data security and storage of records

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.

In particular:

- 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
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals
- Staff are **not** permitted to use portable devices and removable media such as laptops and USB devices to transport sensitive or personal information. All staff are issued with secure logins to enable remote login to the school network to work on school documents off site
- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our **Online Safety, Online Security and Acceptable Use Policies**)
- 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)

15. Disposal of records

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.

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.

16. Personal data breaches

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

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

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:

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

17. Training

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

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

18. Monitoring arrangements

This policy will be reviewed every **2 years** and shared with the full governing board.

19. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Child Protection and Safeguarding Policy
- Acceptable Use Policies
- Online Safety Policy
- Online Security Policy
- Records Management Policy
- Staff Photo Policy
- Remote Learning Policy

Appendix 1: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the Headteacher who will decide if the matter needs to be referred to the DPO. If a decision is taken not to notify the DPO because the reported potential breach does not in fact breach any data protection regulations, the Headteacher will ensure that it is logged in the log saved on the school network at **Y:\GDPR Breaches (Secure)**
- If notified by the Headteacher, 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:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- 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 within the school network 'Y' Drive (Admin) at **Y:\GDPR Breaches (Secure)**
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page](#) of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
 - 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
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - 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
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. 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
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - 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
- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
- Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored **within the 'Y' Drive (Admin) – GDPR Breaches (Secure)**
This will ensure that only authorised staff can gain access to the records saved in this folder.

- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.
- The DPO and headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches.

Actions to minimise the impact of data breaches

We set out below the steps we might take to try to mitigate the impact of different types of data breach if they were to occur, 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.

Special category data (sensitive information) being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it.
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its local safeguarding partners

Other types of breach could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong pupils or families

Appendix 2: Job Description – Data Protection Officer (DPO)

Job Description - Data Protection Officer (DPO)

General information

Location: Corbets Tey School (Main Site and the Avelon Post 16 Provision)

Reporting to: Emma Allen (Headteacher)

Purpose

The DPO is responsible for monitoring compliance with current data protection law, and has the knowledge, support and authority to do so effectively. They oversee the school's data protection processes and advise the school on best practice.

Key responsibilities

To:

- Consult and advise the school about obligations under current data protection law, including the General Data Protection Regulation (GDPR)
- Monitor that key messages about GDPR and data protection are communicated to school staff
- Develop an in-depth understanding of the school's processing operations, information systems, data security processes and needs, and administrative rules and procedures
- Monitor the school's compliance with data protection law, by:
 - Scrutinising the information provided by the school to identify data processing activities
 - Analysing and checking the compliance of data processing activities
 - Informing, advising and issuing recommendations to the school
 - Ensuring they remain an expert in data protection issues and changes to the law, attending relevant training as appropriate
- Ensure the school's policies are followed, through monitoring that
 - There are appropriate responsibilities assigned to individuals
 - Awareness-raising activities take place in the school
 - Staff training is carried out regularly
 - Local authority data protection audits take place and that action plans are followed
- Advise on and assist the school with carrying out data protection impact assessments, if necessary
- Act as a contact point for the Information Commissioner's Office (ICO), assisting and consulting it where necessary, including:
 - Helping the ICO to access documents and information
 - Seeking advice on data protection issues
- Act as a contact point for individuals whose data is processed (for example, staff, students and parents), including:
 - Responding to subject access requests
 - Responding to other requests regarding individuals' rights over their data and how it is used
- Take a risk-based approach to data protection, including:

- Prioritising the higher-risk areas of data protection and focusing mostly on these
- Working with the school on if/when it should conduct an audit, which areas staff need training in, and what the DPO role should involve
- Report to the governing board on the school's data protection compliance and associated risks
- Respect and uphold confidentiality, as appropriate and in line with data protection law, in carrying out all duties of the role
- Undertake any additional tasks necessary to keep the school compliant with data protection law and be successful in the role

- Work with key school staff to ensure that they:
 - Maintain a record of the school's data processing activities
 - Work with external stakeholders, such as suppliers or members of the community, on data protection issues
 - Take responsibility for fostering a culture of data protection throughout the school
 - Work closely with other departments and services to ensure GDPR compliance

Notes for internal candidates

Internal staff members may take on this role, but before expressing an interest should be aware that the DPO must:

- Be a senior member of staff, reporting to the board of governors
- Have a role which is compatible with the DPO role, in terms of time and workload
- Not have any conflicts of interest between their current role and the DPO role

Person Specification

| Criteria | Desirable Qualities |
|-----------------------------|---|
| Qualifications | <ul style="list-style-type: none"> • Background in information security, data protection or IT desired • Educated to degree level, or equivalent professional experience • Relevant data protection qualification desired |
| Experience | <ul style="list-style-type: none"> • Professional experience of data protection law • Experience of managing data protection compliance, particularly responding to subject access requests |
| Skills and knowledge | <ul style="list-style-type: none"> • Knowledge of data protection law • Knowledge of information security and data processing principles and good practice • An understanding, and prior use of the following systems: <ul style="list-style-type: none"> ○ SIMS • Excellent communication skills • Excellent teamwork and interpersonal skills, with proven ability to maintain relationships across a school or other organisation • Ability to explain complex data protection and information security information to a non-specialist audience |
| Personal qualities | <ul style="list-style-type: none"> • Detail-oriented • Ability to prioritise tasks effectively • Ability to work independently and autonomously with minimal supervision • Commitment to maintaining confidentiality at all times |