Data Protection Policy

The Cottesloe School

Policy Type:	Statutory
Reviewed by:	Nicola Hulland (Business Manager), Mark Watson (Link Governor) and Carolyn Stirk (Policies Governor)
Date:	June 2024
Approved by:	Full Governors Meeting - 16.06.2024
Last reviewed:	June 2018
Next review:	Annually

Contents

1. Aims

The Cottesloe School aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

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:

UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020

Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

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

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

- This policy should be read in conjunction with the school safeguarding policy and Keeping Children Safe In Education https://www.cottesloe.bucks.sch.uk/about/policies

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: ● Name (including initials) ● Identification number ● Location data ● Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: ● 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	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.
Data subject	The identified or identifiable individual whose personal data is held or processed.

TERM	DEFINITION
Data controller	A person or organisation that determines the purposes and the means of processing personal data.
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 and carers, pupils, staff, governors, visitors and others, and therefore is a data controller.

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

5. Roles and responsibilities

This policy applies to **all staff** employed by the school, volunteers, and to external organisations or individuals working on its 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, and the board themselves, complies with all relevant data protection obligations.

5.2 Data protection officer (DPO)

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.

They will provide an annual report of their activities directly to the governing board 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 Service Level Agreement

The school's DPO is Nicola Cook and is contactable via: nicola@schoolsdpo.com as this service is outsourced. In school the Business Manager is the DPO lead(DPL) and all enquiries should be referred in the first instance to them.

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 DPL 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 UK

  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 UK 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 1 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 or another person i.e. 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 (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

- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet 1 of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) 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/carer when appropriate in the case of a pupil) 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 the school first collects personal data directly from individuals, it will provide them with the relevant information required by data protection law.

The school will always consider the fairness of data processing. It 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.

7.2 Limitation, minimisation and accuracy

The school 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 the school wants 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.

The school 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 record retention schedule.

8. Sharing personal data

The school 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 pupil or parent/carer that puts the safety of our staff (including volunteers and contractors), visitors or other pupils 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 pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK 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

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 pupils, staff (including volunteers and contractors) or visitors.

Where we transfer personal data internationally, we will do so in accordance with UK 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 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 pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, the school:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made by them

- 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)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or consists of large volumes of data. We will inform the individual of this within 1 month, and explain why the extension is necessary

The school 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 pupil 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 the school refuses 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 that 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 (unless a Court orders otherwise) to free access to their child's educational record (which includes most information about a pupil) 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 pupil 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 pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Biometric recognition systems

Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

The school uses pupil's biometric data as part of the cashless catering system. Fingerprints are used to identify a pupil so they can pay for meals without cash. The school complies with the requirements of the Protection of Freedoms Act 2012.

The school will get written consent from at least 1 parent or person with parental responsibility before any biometric data is taken from their child and first process it.

Parents/those with parental responsibility and pupils have the right to choose not to use the school's biometric system. In these circumstances the school provides access to their food account through alternative means. This is usually a four-digit unique code. Consent may be withdrawn, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil 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 parent(s)/person(s) with parental responsibility.

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

The school uses CCTV in various locations around the school site to ensure it remains safe, and to prevent and detect crime. It will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

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 the Site Manager. Enquiries about the use of CCTV data should be made to the Assistant Headteacher - Cottesloe Character

See the schools CCTV policy

13. 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/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils 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/carer and the pupil.

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

Any photographs and videos taken by parents/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 pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils 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.

14. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The Cottesloe School recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, The Cottesloe School will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

15. 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 a record of attendance

- Encouraging use of mailing lists and mail merge when sending emails to multiple recipients. Where this is not possible, the 'Bcc' field should be used instead. The use of the 'Cc' field should be discouraged.

- 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 UK, where different data protection laws may 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

16. 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, 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. Return of the data to site will be monitored and any data not shown as returned within five working days will be investigated.

- 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 are reminded that they should not reuse passwords from other sites, use easily guessed passwords (e.g. Default1234, etc.) share passwords with anyone else

- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment. *See the school's online safety policy and acceptable use of IT policy* 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)

17. 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.

18. 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, The school will report the data breach to the ICO within 72 hours after becoming aware of it. 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 pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

19. 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.

20. Monitoring arrangements

The DPL is responsible for monitoring and reviewing this policy.

This policy will be reviewed every two years and approved by the full governing board.

Note: the annual review frequency here reflects the Department for Education's recommendation in its advice on statutory policies.

21. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Published Guide to Information
- E Safety Policy
- CCTV policy
- Acceptable use of IT
- Report a Data Breach
-

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO) and the model data breach procedure produced by the school appointed specialist DPO Nicola Cook from Schools DPO

1. Introduction

This data breach response plan is an appendix to our school's Data Protection Policy which it should be read in conjunction with. If you have any queries, please contact The Business Manager our Data Protection Lead in the first instance.

The General Data Protection Regulation (GDPR) defines a personal data breach as:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

A breach of personal data is a type of security incident and falls into one of three categories:

- "Confidentiality breach" - an unauthorised or accidental disclosure of, or access to, personal data
- "Integrity breach" - an unauthorised or accidental alteration of personal data
- "Availability breach" - an accidental or unauthorised loss of access to, or destruction of personal data.

A breach may concern the confidentiality, integrity and availability of personal data at the same time, or any combination. It can be the result of both accidental and deliberate causes.

Some examples of personal data breaches include:

- access by an unauthorised third party (including the malicious acts of hackers and scammers)
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing/mobile devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data, e.g. when it has been encrypted by ransomware, or accidentally lost or destroyed (including natural disasters such as fire and flood).

Under the GDPR any breach of personal data requires mandatory notification to our supervisory authority, the Information Commissioner's Office (ICO); unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.

When a Breach of Personal Data Occurs

As soon as the school is aware* that a breach of personal data has occurred, we will immediately seek to contain the incident and also assess the risk to the rights and freedoms of the individual(s) involved.

***Awareness of a breach occurs when we have a reasonable degree of certainty that a breach has occurred.**

The GDPR requires us to use our resources to ensure we are 'aware' of a data breach in a timely manner. In some cases it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised.

A data incident/breach may occur during school holidays when the school is closed or there are a reduced number of staff available.

The school will ensure that all members of staff have the contact details of the Data Protection Lead (The School Business Manager, DPL and the schools Data Protection Officer ,Nicola Cook DP) so that any incident/breach can still be dealt with appropriately. These contact details are also included in our Data Protection Policy and Privacy Notices, which are available on our website.

3. Assessment of Risk

The risk from a breach is assessed on a case by case basis and both the severity of the potential impact on the rights and freedoms of the individuals and the likelihood will be considered.

When assessing the risk to individuals as a result of a personal data breach we will consider:

- The type of breach
- The nature, sensitivity and volume of the personal data
- How easy it is to identify individuals
- The severity of consequences for individuals
- Special characteristics of the individual, e.g. if they are children
- Any special characteristics of our school
- The number of affected individuals.

A breach is likely to result in a risk to the rights and freedoms of individuals if it could result in physical, material or non-material (e.g.emotional) damage. In particular:

- Loss of control over personal data
- Limitation or deprivation of individuals' rights
- Discrimination
- Identity theft or fraud
- Financial loss
- Damage to reputation
- Unauthorised reversal of pseudonymisation
- Loss of confidentiality of personal data protected by professional secrecy
- Any other significant economic or social disadvantage.

Where special category data* is involved, the GDPR states that such damage should be considered to be likely to occur.

**Special category data is data that is considered more sensitive and requires greater protection: racial or ethnic origin, political opinion, religion or philosophical beliefs, trade union membership, genetic data, data concerning health or sex life, or biometric data used for identification purposes. Data relating to criminal convictions is afforded similar special protection.*

4. Notification to the ICO

As a result of this assessment, if the school believes that there is a risk to the rights and freedoms of the individual(s), we will notify the Information Commissioner's Office, as required under the GDPR. If we are in any doubt, we will always err on the side of caution and notify the ICO.

Where we assess a breach is reportable to the ICO, we must make this report without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach.

As a minimum, we must include in our notification a description of the nature of the personal data breach including ,where possible::

- Categories and approximate number of individuals concerned
- Categories and approximate number of personal data records concerned
- Name and contact details of the DPO
- description of the likely consequences of the personal data breach
- description of the the measures that have been;or will be taken, to deal with the breach and mitigate any possible adverse effects on the individuals concerned

The GDPR makes no allowance in the statutory reporting timescale of 72 hours for breaches that occur during school holidays.

Therefore, it is important that staff contact the school Data Protection Lead and or the DPO as soon as possible.

5. Communication to affected individuals

Where a data breach is likely to result in a high risk to the rights and freedoms of individuals, we will notify affected individuals as soon as possible. We will provide:

- A description of the nature of the breach
- The name and contact details of the DPO and/or Data Protection Lead
- A description of the likely consequences of the breach
- A description of the measures taken or proposed to be taken by the school to address the breach and mitigate any possible adverse effects.

We will also consider what specific advice we can provide to individuals to help them protect themselves, such as resetting passwords where access credentials have been compromised.

6. Roles and Responsibilities

All Staff - if any member of staff believes a breach of personal data has occurred, or might have occurred, they must immediately notify the Data Protection Lead.

At The Cottesloe School this is The School Business Manager(ext 210 email:nhulland@cottesloe.bucks.sch.uk) who will liaise with the Data Protection Officer who is

Nicola Cook, Schools DPO Ltd: 01296 658502, nicola@schoolsdpo.com.

If members of staff receive personal data sent in error they must alert the sender and the Data Protection Lead as soon as they become aware of the error.

The Data Protection Lead, with the support of colleagues, will investigate the report, and determine whether a breach has occurred. To decide, they 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

The Data Protection Lead(DPL) will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.

In discussion with the DPL, the DPO will assess the potential consequences of the breach and advise whether the breach needs to be reported to the ICO.

If the breach is likely to be a risk to the people's rights and freedoms, the DPO will notify the ICO.

Where a breach is likely to result in a high risk to people's rights and freedoms, the Data Protection Lead will promptly inform, in writing, all individuals whose personal data has been breached.

This notification will include:

- 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 individuals concerned.
- The Data Protection Lead will document each breach,irrespective of whether it is reported to the ICO and ensure a record is kept in the Data Breach Register

Data Breach notification form which forms the basis of the Data Breach register

7. Actions to minimise the impact of data breaches

The type of action taken will depend on the nature of the breach, but could include the following (this list is not exhaustive):

- Attempting to recover lost equipment
- Remotely wiping electronic devices
- Using of back-ups to restore lost/damaged/stolen data
- Changing entry codes or IT system passwords
- Attempting to recall emails containing personal information that are sent to unauthorised individuals
- Requesting personal data received in error is deleted and written confirmation is provided that the information has been deleted, and not shared, published, saved or replicated in any way
- Carrying out internet searches to check information hasn't been made public. If it has, asking the publisher/website owner/administrator to remove and destroy the information

- Briefing staff in case of phishing enquiries for further information on affected individuals
- Notifying the Governors and Local Authority

The school will review the effectiveness of any actions taken and amend them as necessary after any data breach. This may include establishing more robust policies and procedures or providing further training for staff.

8. Accountability and Record Keeping

The School records all breaches of personal data regardless of whether they are reported to the ICO. This helps to demonstrate compliance with the GDPR under its principle of accountability. It also ensures the school has records should the ICO wish to see them.

Data Breaches are recorded using the Data Breach notification form. The information collected on this forms the basis of the schools data breach record. It includes the following information:

- A summary of the facts
- The type and quantity personal data involved
- details of the cause of the breachand the anticipated impact on the individuals whose data is involved
- Actions taken to contain the breach as well as to mitigate any possible adverse effects
- Any actions taken to prevent future breaches and lessons learned