Mayfield School

Data Protection Policy

Believe. Achieve. Succeed.

Respectful, Resourceful, Responsible, Reflective, Resilient, Ready

Our School Vision

Our vision is to create a family ethos that raises aspirations and makes a real difference to the life chances of our young people.

Our mission

All stakeholders, together, will create an environment of respect and inclusion where all young people are valued, supported, inspired and future ready.

Approved by: Personnel and Finance Committee	**Date:** 10th May 2023
Review frequency: 2 years	**Statutory requirement:** No
Last reviewed: May 2023	**Next review due:** May 2025

Contents

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, 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 meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

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	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.

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

The school is registered with 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 Body

The governing body 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 developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing body and, where relevant, report to the body 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.

Our DPO is Matthew Stedman and is contactable via stedmanm@mayfield.portsmouth.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 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 one 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 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 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 record retention schedule.

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 pupil or parent/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 pupils – for example, IT companies. 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

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 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 pupils in our Primary Section may 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.

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 in our Senior Section 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 a subject access request

Verifying the Identity of a Requester

Mayfield School is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Unless personally known, a requester should provide their address and valid evidence to prove their identity by production of two or more of the following:

- Current UK/EEA Passport;
- UK Photocard Driving Licence (Full or Provisional);
- EEA National Identity Card;
- Full UK Paper Driving Licence;
- State benefits entitlement document*;
- State pension entitlement document*;
- HMRC Tax Credit document*;
- Local Authority benefit document*;
- HMRC Tax Notification document;
- Financial statement issued by bank, building society or credit card company+;
- Judiciary document, such as a Notice of Hearing, Summons or Court Order;
- Utility bill for supply of gas, electric, water or telephone landline+;
- Most recent mortgage statement;
- Most recent Council Tax Bill or statement;
- Current Council rent card;
- Current Council Tenancy Agreement;
- Building Society passbook, which shows a transaction in the last 3 months and the address.

Documents marked with a * must be dated in the past 12 months and documents marked with a + must be dated in the past 3 months.

If Mayfield School is not satisfied as to the identity of the requester then the request will not be completed, to avoid the potential for an inadvertent disclosure of personal data resulting in a data breach.

Fee for Responding to Requests

Mayfield School will usually deal with a SAR free of charge. Where a request is considered manifestly unfounded or excessive, a fee may be requested;

Alternatively, Mayfield School may refuse to respond to the request. If a request is considered to be manifestly unfounded or unreasonable, Mayfield School will inform the requester why this is considered the case;

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances, a reasonable fee will be charged taking into account the administrative costs of providing the information.

Time Period for Responding to a SAR

Mayfield School has one month to respond to a SAR. This will run from the later of:

- the date of the request
- the date when any additional identification (or other) information requested is received
- payment of any required fee.

In circumstances where Mayfield School is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to

their identity, and in the case of a third party requester the written authorisation of the data subject has been received (see below in relation to sharing information with third parties).

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request and will be defined by the DPO on a case by case basis.

Where a request is considered sufficiently complex as to require an extension of the period for response, Mayfield School will notify the requester within one calendar month of receiving the request, together with reasons as to why this is considered necessary.

A request may be received during or less than one month prior to a school holiday. Where a request is made prior to a holiday period, Mayfield School will seek to respond prior to that holiday commencing, however, where this is not possible then Mayfield School will inform the requester that this is the case.

Form of Response

A requester can request a response in a particular form. Where a request is made by electronic means then, unless the requester has stated otherwise, the information should be provided in a commonly readable format.

In accordance with the Education (Pupil Information) (England) Regulations 2005, the School shall make a pupil's educational record available for inspection by the parent, free of charge, within fifteen school days of the receipt of the parent's written request for access to that record;

Withholding Information

There are circumstances where information can be withheld pursuant to a SAR. These are specific exemptions and requests should be considered on a case-by-case basis. Where the information sought contains the personal data of third-party data subjects then Mayfield School will:

- Consider whether it is possible to redact information so that this does not identify those third parties, taking into account that it may be possible to identify third parties from remaining information;
- If this is not possible, consider whether the consent of those third parties can be obtained; and if consent has been refused, or it is not considered appropriate to seek that consent, then to consider whether it would be reasonable in the circumstances to disclose the information relating to those third parties. If it is not then the information may be withheld;
- As far as possible, Mayfield School will inform the requester of the reasons why any information has been withheld;
- Where providing a copy of the information requested would involve disproportionate effort, Mayfield School will inform the requester, advising whether it would be possible for them to view the documents at the school or seeking further detail from the requester as to what they are seeking, for example key word searches that could be conducted, to identify the information that is sought.
- In certain circumstances, information can be withheld from the requester, including a data subject, on the basis that it would cause serious harm to the data subject or another individual. If there are any concerns in this regard then the DPO should be consulted.

Process for Dealing with a Subject Access Request

When a subject access request is received, Mayfield School will:

- Notify the DPO who will be responsible for managing the response;

- Acknowledge receipt of the request and provide an indication of the likely timescale for a response within 5 working days;
- Take all reasonable and proportionate steps to identify and disclose the data relating to the request;
- Never delete information relating to a subject access request, unless it would have been deleted in the ordinary course of events – it is an offence to amend or delete data following receipt of a SAR that would not have otherwise been so amended or deleted;
- Consider whether to seek consent from any third parties which might be identifiable from the data being disclosed;
- Seek legal advice, where necessary, to determine whether Mayfield School is required to comply with the request or supply the information sought;
- Provide a written response, including an explanation of the types of data provided and whether and as far as possible for what reasons any data has been withheld;
- Ensure that information disclosed is clear and technical terms are clarified and explained.

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 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

Where we use pupils' biometric data as part of an automated biometric recognition system for example, the school meals payments system in the senior section, we will comply with the requirements of the Protection of Freedoms Act 2012.

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

Parents/carers and pupils 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. For example, pupils can be provided with a pin number to pay for their school meals.

Parents/carers and pupils can withdraw consent, 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)/carer(s).

Where staff members or other adults use the school's biometric system, 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

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.

Mayfield School has a separate CCTV Policy which is available on the school website.

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 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 parent/carer and pupil.

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 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. 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
- 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, type of 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

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
- Passwords that are at least 10 characters long containing letters, numbers and special characters 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
- 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
- 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. Data Protection during Remote Learning and Home Working

It is essential that best data protection practice is still enforced while staff and pupils are working or learning remotely from home. Data Protection issues to be considered include:

- Pupils and staff only visiting trusted sites, and avoid downloading or opening any attachments from sources they do not recognise.
- Staff should also be aware that they must avoid sharing a device at home, unless there is the appropriate access control to the areas they use for work. While school staff should already have been trained in data protection and therefore should know what is safe to access and what is not, other family members may be less vigilant.
- Be mindful of the websites and platforms that we ask pupils to access. If a system can be used which involves no data to be entered, no registration and no file downloads, and is within a secure website which displays "https", then it should be safe to use.

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, we will report the data breach to the ICO within 72 hours after becoming aware of it.

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 DPO is responsible for monitoring and reviewing this policy.

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

21. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Mayfield School Privacy Notice
- E-Safety and Use of Social Media Policy
- CCTV Policy
- Guidance around Online Teaching

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

The purpose of this policy is to ensure a standardised approach to managing and reporting data security incidents and data breaches, to ensure that they are dealt with speedily and efficiently, with consistency, to keep our process open and transparent, to keep damage and distress to a minimum and reduce the likelihood of reoccurrence by implementing appropriate measures.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Officer (DPO). Any potential breach should be reported promptly, as soon as the staff member is able, as the DPO has to report any serious breaches to the ICO within 72 hours.

When reporting an incident, members of staff must give the DPO sufficient information to determine whether a breach has occurred and how serious it is. Where practicable, they should identify:

- The date and time of the incident;
- A description of the incident;
- The number of individuals (data subjects) who are affected;
- The details of any school IT systems, or third party systems, that are involved;
- Details of any actions that have been taken to mitigate/minimise the effect on the data subjects;
- The details of any contractors, or sub-contractors, who are involved.

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.

If the breach is serious, the DPO will alert the headteacher and the chair of governors. Where appropriate, the DPO will also inform Portsmouth City Council.

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).

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

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 nonmaterial damage (e.g. emotional distress), including through:

- Loss of control over their data;
- Discrimination;
- Identify theft or fraud;
- Financial loss;

- Unauthorised reversal of pseudonymisation (for example, key-coding);
- Damage to reputation;
- Loss of confidentiality;
- Any other significant economic or social disadvantage to the individual(s) concerned.

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

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

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 the school's cloud computer system.

Mayfield School believe in the importance of identifying the root cause of any potential incident/breach in order to ensure our internal systems are robust and that we can take action in order to prevent a reoccurrence.

The Data Protection Officer for Mayfield School is Matthew Stedman, Director of Business Operations, and he can be contacted on 02392693432 or via email stedmanm@mayfield.portsmouth.sch.uk