

Forest Fields Primary and Nursery School



Data Protection Policy 2025

DATE: *September 2025*

To be approved at the meeting of the Governing Board held on: 23rd September 2025

Signed: *James Verran*

Position: *Chair of Governors*

Date to be reviewed: *September 2026*

Contents

1.Introduction	3
2. Aim	4
3. Legislation and guidance	4
4. Definitions	4
5. The data controller	6
6. Processing of information	6
7. What counts as personal information	7
8. Processing of special categories of personal information	7
9. Roles and responsibilities	7
10. Collecting personal data	9
11. Sharing personal data	9
12. Subject access requests and other rights of individuals	10
13. Parental requests to see educational records	12
14. Request from other agencies for personal information	13
15. Fair obtaining/processing	13
16. Data uses and purposes	14
17. Data incident reporting / Data breach	14
18. Data quality and retention	15
19. Records of processing activities	15
20. Data security and storage of records	15
21. Disposal of records	16
22. CCTV	16
23. Photographs and videos	17
24. Training	17
25. Links with other policies	18
Appendix 1: Personal data breach procedure	19

Forest Fields Primary School “the school” recognises that this policy is, by its very nature, complex. If you would like an explanation of any of the terminology used, or to understand how it may affect you, please speak to a member of the school office team or ask to see our Data Protection Officer.

Any web-links contained in this policy are correct and working at the time of approval. If you find a link that doesn't work please let our school office team know. Please email us at Admin@forestfields.nottingham.sch.uk.

1. Introduction

Forest Fields Primary and Nursery School aims to ensure that personal information is treated in a lawful, fair and transparent manner. The lawful and correct treatment of personal information is extremely important in maintaining the confidence of those with whom the school deals and in achieving its objectives. This policy sets out the basis on which we shall process any personal data from our students, their parents/carers, staff, visitors and other parties from whom data is collected.

We, and therefore any person who handles personal data on behalf of the school, fully endorse and adhere to the data protection principles set out in Article 5 of the GDPR and sections 83-89 DPA 2018 as below and shall be responsible for and be able to demonstrate compliance with the seven data protection principles.

These data principles are that personal information shall be:

- processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**)
- collected for specified explicit and legitimate purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes; (**purpose limitation**)
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; (**data minimisation**)
- accurate and where necessary kept up to date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**accuracy**)
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required to safeguard the rights and freedoms of the data subject (**storage limitation**)
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**integrity and confidentiality**)
- kept in a responsible manner and compliance is demonstrated by ensuring there are appropriate measures and records in place along with compliance of all data principles (**accountability**)

2. Aim

Our school aims to ensure that all the personal data we hold is collected, stored and processed in accordance with the [General Data Protection Regulation \(GDPR\)](#) and the provisions of the [Data Protection Act 2018 \(DPA 2018\)](#).

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

To achieve this aim the school will:

- Provide adequate resources to support an effective approach to data protection.
- Respect the confidentiality of all personal information irrespective of source.
- Publicise the school's commitment to Data Protection.
- Compile and maintain appropriate procedures and codes of practice.
- Promote general awareness and provide specific training, advice and guidance to its staff at all levels to ensure standards are met.

Monitor and review compliance with legislation and introduce changes to policies and procedures where necessary.

3. Legislation and guidance

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#) and the ICO's [code of practice for subject access requests](#). 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. The policy also recognises the requirements of the Regulatory Reform (Fire Safety) Order 2005, which requires us to ensure the identification and safe evacuation of all relevant persons on our premises.

The UK left the EU on 31st January 2020, but the GDPR continue to apply.

4. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, 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.
Consent	Any freely given, specific, informed and unambiguous indication of wishes, by a statement or clear affirmative action which signifies agreement to the processing of data.
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.
Educational records	The right of access to any record of information which relates to a, pupil and therefore includes any education, health and care plan and any personal education plan. Educational records do not include information which is processed by a teacher solely for the teacher's own use such as a lesson plan.
Subject Access Request	The right to the personal data by the pupil or parent/carer of the pupil

5. 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 as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

6. Processing of information

The school, through appropriate management controls will, when processing personal information about any individual:

- Observe fully the conditions regarding the collection and use of information and meet the school's legal obligations under the UK GDPR and the Data Protection Act 2018.
- Collect and process appropriate information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirement.
- Ensure that the individual about whom information is held can exercise their rights under the Act unless an exemption applies for example in relation to education data, including the right:
 1. to be informed that processing is being undertaken
 2. to prevent processing in certain circumstances
 3. to correct, rectify, block or erase information, which is regarded as incorrect information
 4. of access to personal information
 5. to erasure
 6. to portability where applicable.

7. What counts as personal information

This is any information held by the school about a living individual, from which that individual can be identified. For example, this includes:

- A name and address or contact details held about pupils, students, parents and staff and their families
- characteristics such as ethnicity, language, nationality, country of birth, free school meals, adopted and fostered
- information attached to a reference number that could be used to identify someone
- a pupil's school record, including achievement, attendance, sickness, necessary health care plan details
- photographs of a child
- financial records relating to a child's parents
- staff employment records

8. Processing of special categories of personal information

The school, through appropriate management controls will, when processing special categories of personal information about any individual:

- Observe fully the conditions regarding the processing of special categories of information as outlined in Article 9 and meet XXX's legal obligations under the UK GDPR and the Data Protection Act 2018. In particular, Schedule 1 Part 4 of the DPA 2018 states that the school must have this policy document in place which explains as below, the procedures for securing compliance with the principles in Article 5 as outlined above.
- Collect and process special categories of data only to the extent that it is needed to fulfil operational needs or to comply with any legal requirement.
- Process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs data, data concerning health or data concerning a natural person or trade union membership and the processing of genetic data biometric data for the purpose of uniquely identifying a natural person.

9. 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.

9.1 Governing body

The School Governors have overall responsibility for ensuring that our school complies with all relevant data protection obligations.

9.2 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 school Governors and, where relevant, report to the Governing 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.

To contact our DPO please email DPO@forestfields.nottingham.sch.uk.

9.3 Headteacher

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

9.4 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

10. Collecting personal data

10.1 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, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed for the **legitimate interests** of the school or a third party
- 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 to ensure the **vital interests** of the individual e.g. to protect someone's life
- 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 which are set out in the GDPR and DPA 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

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

10.2 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. 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 [*Information and Records Management Society's toolkit for schools*](#).

11. Sharing personal data

We will not normally share personal data with anyone else, but may do so 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 data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, 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, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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

12. Subject access requests and other rights of individuals

The school will process requests for access to personal information in line with the relevant sections of the UK GDPR and the Data Protection Act 2018.

12.1 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

- 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

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

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

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

If all information has been received, and the request is a valid subject access request, the school will acknowledge the request and process the request within 30 days from receipt; unless the request is particularly large and complex in which case the time can be extended for two months.

12.2 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 at our school 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.

12.3 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
- 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 numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records

- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

12.4 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, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- 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.

13. Parental requests to see the educational record

The Education (Pupil Information) (England) Regulations 2005 allow parents/carers access to the official education records of their children. The school will make a pupil's educational record available for inspection or provide a copy of the record within 15 days of a valid written request by a parent/carer. Any charges for copying will not exceed the cost of supply.

The school may refuse to disclose information under the Pupil Information Regulations where:

- The school would have no right to disclose the information to the pupil under the UK GDPR and DPA 2018.
- The information might cause serious harm to the physical or mental health of the pupil or another individual.

When providing information to an individual the school will seek to verify the individual's identity.

The school will not disclose anything on a pupil's record that would be likely to cause serious harm to their physical or mental health or that of anyone else. Therefore, those creating such records will make sure this kind of information is kept separate from the pupil's other records. Where there is a doubt or statutory requirements conflict staff should seek advice in the first instance from the Data Protection Officer.

14. Requests from other agencies for personal information

- Requests from any external agency will be processed in accordance with the UK GDPR and Data Protection Act 2018.
- The staff member responsible for dealing with such requests will ensure that any disclosure made without the consent of the parent/carer is done in accordance with the data protection and other relevant legislation, taking account of an individual's rights as enshrined in the Human Rights Act 1998. Relevant, confidential information should only be disclosed to:
 - other members of staff on a need to know basis
 - relevant Parents/Carers;
 - other authorities if it is necessary in the public interest, e.g. prevention of crime;
 - other authorities, such as the Local Authority and schools to which a pupil may move, where there are legitimate requirements (DfE leaflet 0015/2000 entitled "Pupil Records and Reports" issued in March 2000 covers Data Protection issues and how and what information should be transferred to other schools. DfES/0268/2002 provides further information).

15. Fair obtaining / processing

Individuals whose information is collected by the school must be made aware at the time of collection of all the processes that data may be subject to. No manual or automatic processing of a pupils personal information will take place unless reasonable steps have been taken to make that individual aware of that processing.

Parents/Carers can also be informed of likely recipients of their information, both internal and external, and also be given details of who to contact in order to query the use or content of their information. The pupils/students and other data subjects will also be informed of the purposes of the processing as well as the legal basis for processing where appropriate.

Information as to how long the information will be kept for, the rights that the parents/carers can exercise with regards to their data and information to enable pupils/students to lodge a complaint with the Information Commissioners Office if

their rights are not met under the UK GDPR and DPA 2018 can be provided on request.

16. Data uses and purposes

All processing of personal data will be for a purpose that is necessary to enable the school to perform its duties and services. Personal information must only be processed in line with those notified purposes.

All personal data will be regarded as confidential and its security protected accordingly. This also applies when information is being processed at members of staff's homes. Information held by the school must not be used for unauthorised non-school purposes. If you become aware of any potential data breach, please contact the DPO immediately.

Personal Information should only be disclosed to persons (internal and external) where their authority to receive it has been explicitly established, e.g. where the information is required by the police for the prevention and detection of crime, or a relevant Information Sharing Agreement is in place. Purposes will include the following:

- Providing education and pastoral care
- Providing activities for pupils/students including trips, clubs and activities
- Safeguarding and promoting the welfare of children
- Providing references for pupils/students and staff
- Providing human resource functions for staff
- Ancillary purposes to education including completing contractual obligations
- Fundraising.

17. Data incident reporting / Data breach

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.

A data breach can be defined as a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorised to do so.

Staff members must notify the Data Protection Officer / Headteacher of any potential data incidents as soon as the incident occurs and in any event within 24 consecutive hours after occurrence. Any reported data incident will be investigated appropriately and actions taken as necessary.

If a member of the public wishes to report a potential incident, they can do this by contacting the Data Protection Officer/ Headteacher directly by phone on 0115 915 6872.

Personal data breaches will be notified to the Information Commissioner's Office within 72 hours of the incident. All staff members will follow the school's Data Incidents and Breaches policy and procedure.

18. Data quality and retention

Information processed should not be excessive or irrelevant to the notified purposes. Information must be held only for so long as is necessary for the notified purposes, after which it should be deleted or destroyed in accordance with the school's Records Management and Retention Policy.

Whenever information is processed, reasonable steps should be taken to ensure that it is up to date and accurate.

19. Records of processing activities

In order to be able to properly and effectively comply with our obligations under the UK GDPR and the DPA2018, the school needs to fully understand what information it holds and where this information is kept. We also need to consider how we keep this information up-to-date and how we know when to dispose of it. The school shall maintain a record of processing which includes the following information:

- The name of the school and the details of the Data Protection Officer
- The purposes of processing as outlined above in this policy document
- Which condition is relied on and in particular, how the processing satisfies Article 5 and 6
- The ownership, governance and maintenance of Information Assets
- A Records Management and Retention Policy
- Whether the personal data is retained and erased in accordance with the policy and if it is not the reason for not following the policy
- Map the flow of data in and out of the school

20. Data Security and storage of records

The school must take all appropriate technical and organisational measures to safeguard against unauthorised or unlawful processing of personal information and against accidental loss, damage or destruction of personal information.

All personal information must be kept secure, in a manner appropriate to its sensitivity and the likely harm or distress that would be caused if it was disclosed unlawfully.

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 seek the agreement of the Headteacher or the DPO.
- The school will follow good practice advice on the use and creation of complex passwords. Staff and pupils are reminded to change their passwords at regular intervals
- 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 our acceptable use 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

21. 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 and/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.

22. 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 our Site Manager. Please email any queries to admin@forestfields.nottingham.sch.uk.

23. 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.

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

Uses may include:

- Within school on notice boards and on the news page of our Weduc communication App, 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 safeguarding policy for more information on our use of photographs and videos.

24. 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.

25. Links with other policies

This Data Protection Policy should be read in conjunction with the following:

- Data Incidents and Breaches Policy
- Freedom of Information Policy
- Remote Access and Mobile Computing Policy
- Subject Access Request Policy
- Acceptable Use policy
- Email Policy
- Mobile Computing Policy
- Safeguarding Policy and Guidance

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 or data processor must immediately notify the DPO
- 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
- The DPO will alert the head teacher and the chair of governors
- 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 non-material 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.

- 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 in our Personal Data Security Beach Log. This is an electronic document maintained by the DPO and store at the school.
- Where the ICO must be notified, the DPO will do this via the '[report a breach](#)' [page of the ICO website](#) within 72 hours. 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. 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
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - 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 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 [set out where you will keep these records – for example, on the school's computer system, or on a designated software solution]

- The DPO and head teacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

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