



2a Vickery Way, Chilwell, Nottingham, NG9 6RY

0115 989 1915

[info@flyinghightrust.co.uk](mailto:info@flyinghightrust.co.uk) 



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 UK data protection law.

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

- \_\_\_\_\_  
\_\_\_\_\_
- \_\_\_\_\_  
\_\_\_\_\_

**Schools that use biometric data insert text below – if not, please delete:**

It meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to our use of biometric data.

**Schools that use CCTV insert – if not, please delete:**

It also reflects the ICO's [guidance](#) for the use of surveillance cameras and personal information.

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





responsibility of data controller to the school business or office manager within each school and to the Trust Operations Manager centrally.

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

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

## 5.1 Governing board

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

## 5.2 Data protection officer

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

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

- 
- 







2a Vickery Way, Chilwell, Nottingham, NG9 6RY



0115 989 1915



info@flyinghightrust.co.uk



www.flyinghighpartnership.co.uk







2a Vickery Way, Chilwell, Nottingham, NG9 6RY

0115 989 1915

[info@flyinghightrust.co.uk](mailto:info@flyinghightrust.co.uk) 

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

Where we use pupils’ biometric data as part of an automated biometric recognition system (for example, pupils and/or staff use finger prints to unlock devices **[amend this example as applicable]**), we will comply with the requirements of the [Protection of Freedoms Act 2012](#).

---

2a Vickery Way, Chilwell, Nottingham, NG9 6RY

 0115 989 1915

 [info@flyinghightrust.co.uk](mailto:info@flyinghightrust.co.uk) 

[www.flyinghighpartnership.co.uk](http://www.flyinghighpartnership.co.uk)

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.

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 sipdpá

2a Vickery Way, Chilwell, Nottingham, NG9 6RY

 0115 989 1915

 [info@flyinghightrust.co.uk](mailto:info@flyinghightrust.co.uk) 

[www.flyinghighpartnership.co.uk](http://www.flyinghighpartnership.co.uk)

- 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.
- 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)

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.

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. 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

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.

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


- 
- 
- 
- 



- 
- 

---

2a Vickery Way, Chilwell, Nottingham, NG9 6RY

 0115 989 1915

 [info@flyinghightrust.co.uk](mailto:info@flyinghightrust.co.uk) 

[www.flyinghighpartnership.co.uk](http://www.flyinghighpartnership.co.uk)

## Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (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
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the Operations Manager or DPO will alert the headteacher and the chair of governors
- The Operations Manager or DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the Operations Manager or DPO with this where necessary, and the Operations Manager or DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The Operations Manager or DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The Operations Manager or DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's [self-assessment tool](#)
- The Operations Manager or DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school/Trust log.
- 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 received



reasons why, and when the Operations Manager or DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- Where the school is required to communicate with individuals whose personal data has been breached, the Operations Manager or Operations Manager or DPO will tell them in writing. This notification will set out:
  - A description, in clear and plain language, of the nature of the personal data breach
  - The name and contact details of the Operations Manager or 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 Operations Manager or DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The Operations Manager or 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 on the school/Trust log.

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

## Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

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

- If special category data is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the Trust Operations Manager or DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the Trust Operations Manager or DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the Trust Operations Manager and/or DPO will contact the relevant unauthorised individuals who received the email, explain that the information



was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The Trust Operations Manager and/or DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The Trust Operations Manager and/or DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach that you might want to consider could include:

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

---

2a Vickery Way, Chilwell, Nottingham, NG9 6RY

 0115 989 1915

 [info@flyinghightrust.co.uk](mailto:info@flyinghightrust.co.uk) 

[www.flyinghighpartnership.co.uk](http://www.flyinghighpartnership.co.uk)