

Fyling Hall School  
Data protection policy

## **Statement of intent**

Schools have direct responsibility for ensuring that they comply with the Data Protection Act (1998) and handle personal data in line with it. Fyling Hall takes its obligations seriously and has a number of policies which support the safe maintenance of – and access to – information about students, staff and parents.

In particular, the Data Protection Act places the following obligations on schools:

- notifying the Information Commissioner's Office (ICO) of the school's register entry
- providing a statement or 'privacy notice' to individuals (such as pupils and parents) whose personal data is being processed or held
- responding to requests for personal data or 'subject access requests' within 40 calendar days

This policy applies to all members of Fyling Hall School (including trustees, staff, students, volunteers, parents/carers, visitors) but is of particular relevance to those people involved with the collection, processing and disclosure of personal data.

## **Our commitments**

Fyling Hall commits to handling data and information in accordance with the eight principles set out in the Data Protection Act.

### **Principle 1: fair obtaining and processing**

We undertake to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which data are held, the likely recipients of the data and the data subject's right of access.

- "processing" means obtaining, recording or holding the information or data or carrying out set operations on the information or data
- "data subject" means an individual who is the subject of personal data or the person to whom the information relates; for example, this may be a student or a member of staff
- "personal data" means data which relates to a living individual who can be identified; for example addresses, telephone numbers, names
- "parent" has the meaning given in the Education Act (1996) and includes any person having parental responsibility or care of a child

### **Principle 2: personal information must be processed for limited purposes**

Fyling Hall's data processing registration entry is available via the Information Commissioner's Office: <https://ico.org.uk/ESDWebPages/Entry/Z5143582>

Registered purposes covering the data held at the school are listed on the school's registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

### **Principle 3: personal information must be adequate, relevant and not excessive**

In order to ensure that the data held about people meets this principle, Fyling Hall may periodically check records to identify missing, irrelevant or seemingly excessive information. We may contact the data subject to verify certain items of data.

### **Principle 4: personal information must be accurate and up to date**

We aim to ensure that all data held is as accurate and up to date as is reasonably possible. It is the responsibility of a data subject to ensure that records are updated as necessary (this can be done via the school office). If a data subject informs the school of a change of circumstances (for example, a new address or telephone number), their records will be updated as soon as is practicable.

Any concerns about the accuracy of your data should be raised with the school office. If a data subject challenges the accuracy of their data, the school will immediately mark the record as potentially inaccurate ('challenged'). It is hoped that any dispute could be resolved informally, but either party may seek independent arbitration. In the event of unresolved challenged data being disclosed, the disclosure must include both versions of the information.

### **Principle 5: personal information must not be kept for longer than necessary**

Data held about individuals will not be kept for longer than is necessary to meet the stated registered purposes. It is the responsible of the Headmaster to ensure that obsolete data are properly erased.

### **Principle 6: processed in line with the data subject's rights**

The Data Protection Act gives individuals rights in respect of the personal data Fyling Hall holds about them. This includes:

- a right to access a copy of their personal data (*see 'Subject access requests' section below for this procedure*)
- a right to object to processing that is likely to cause, or is causing, damage or distress
- a right to prevent processing for direct marketing
- a right to object to decisions being taken by automated means
- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed (*see Principle 4 above for procedure*)
- a right to claim compensation for damages caused by a breach of the Act

Any data subject who wishes to discuss their rights in more detail may contact the Headmaster via the school office.

### **Principle 7: personal information must be secure**

We use a variety of methods to ensure that personal data is kept secure including:

- physical security (building keycodes; building alarms; locked cabinets; restricted access to the server room; all visitors must display a visitors badge; unique visitor login with restricted access to network; access to school network via password only;)
- logical security (backing up computer systems; installation of security software; only authorised users can access computers)
- procedural security (training provided to new users; Acceptable Use agreement; staff are aware of their obligations to keep data safe; paper documents are shredded)

### **Principle 8: personal information must not be transferred to other countries without adequate protection**

As an international school, there may be circumstances when personal data is transferred to a country outside the European Economic Area (EEA) or to a country which the European Commission does not consider provides 'adequate protection'. In such circumstances, all options to avoid sending personal data will first be explored. If it is deemed necessary to transfer personal data to a non-EEA country, the consent of the data subject must be requested and given.

## **Whole school responsibility for data protection**

Within Fyling Hall all members of staff and students are responsible for data protection; responsibilities for each group include:

### **Trustees**

Trustees are responsible for the approval of the data protection policy and for reviewing the effectiveness of the policy. This will be carried out by the trustees receiving regular information about any requests for information made under the Data Protection Act and any incidents relating to data protection. A member of the Governing Body has taken on the role of the Information & Technology trustee. The role of the Information & Technology trustee will include:

- regular meetings with the Head of ICT or Designated Senior Lead
- regular monitoring of data protection incident logs
- reporting to relevant trustees

### **Students**

Students must, at all times, respect the privacy of others. This presumption forms the basis of the ICT Acceptable Use policy. The responsibilities of students include:

- compliance with the student's ICT Acceptable Use policy and agreement, which students must agree to each time they use school ICT equipment either in the school or when remotely connected to the wireless network
- not forwarding private data without permission from the author
- not supplying personal information about themselves or others via the web, email or instant messaging
- reporting any data protection issues or incidents to a teacher, member of staff or parent
- taking responsibility for their own actions when using the internet and communications technologies which use or store personal data
- taking responsibility for the protection of their own network account and not divulging passwords to anybody including members of staff

### **All staff**

Staff must, at all times, respect the privacy of students and colleagues. This presumption forms the basis of the ICT Acceptable Use policy. Please note that individual members of staff can be personally liable under the Data Protection Act, including claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this policy will be treated as a disciplinary matter, and serious breaches could lead to dismissal. The responsibilities of staff include:

- compliance with the staff ICT Acceptable Use policy and agreement, which staff must agree to each time they use the school ICT equipment either in the school or when remotely connected to the wireless network
- awareness of own responsibilities for the collection, processing and disclosure of personal data within these guidelines
- maintaining the security of personal data, both that held in hard copy and electronically
- reporting any data protection issues or incidents to the Designated Lead

### **Designated lead**

Additional responsibilities above those applicable to all staff lie with a designated lead. These additional responsibilities include:

- investigating any concerns raised about the accuracy of someone's data and immediately marking the record as potentially inaccurate ('challenged')
- ensuring that obsolete data are properly erased
- logging details of all subject access requests
- processing, and responding to, subject access requests within 40 calendar days
- processing, and responding to, requests for personal data (for example, court orders or police requests)
- logging details of all other authorised disclosures of data
- ensuring that data about third parties is removed from data disclosed to data subjects or other authorised recipients

- providing information contained within the data protection logs to trustees
- escalating any concerns about data protection to the designated trustee with responsibility for e-safety

## **Contractors**

There may be occasions when external contractors (for example, computer engineers) have unavoidable access to personal data. In such circumstances, their responsibilities include:

- signing a statement agreeing not to disclose data outside of the school
- reporting any data protection issues or incidents to the designated lead

## **Subject access requests**

The Data Protection Act gives all data subjects the right to access their own personal data. Anyone requesting access to their personal data must do so in writing using the formal template included in this policy. Fyling Hall will respond within 40 calendar days of receiving the completed request and identification documents. In most circumstances, a copy of the relevant information will be provided to you. A fee will be charged to cover the administrative costs to Fyling Hall of fulfilling a request. Where appropriate, Fyling Hall may offer a data subject supervised access to their original records.

Where the request is made by a pupil they will directly receive a copy of their data unless it is clear that they do not understand the nature of the request (in which case, the request will be referred to their parent). A request made by a parent on behalf of their child will be fulfilled if Fyling Hall considers this to be in the best interests of the child. If we are confident that the child can understand their rights, then we will respond to the child rather than to the parent. Please note that the information provided to you may be redacted, for example if it contains personal data about a third party.

## **Authorised disclosures**

In certain circumstances, Fyling Hall may be required to disclose personal data without the data subject's explicit consent in accordance with Section 29 of the Data Protection Act. This may include sharing information with other professionals working within, or with, the school who need the information in order to do their job.

Only authorised staff (**Members of the SMT & the Assistant Bursar**) are permitted to make external disclosures of personal data, which will be assessed on a case-by-case basis. Fyling Hall will not disclose any data which it considers would cause serious harm to anyone's mental or physical health. These circumstances are limited to disclosing:

- pupil data to authorised recipients related to education and administration necessary for Fyling Hall to perform its statutory duties and obligations

- pupil data to authorised recipients in respect of a child's welfare, health and safety (for example, the police)
- pupil data to parents in respect of their child's progress, achievements, attendance, attitude and demeanour within school
- staff data to relevant authorities (for example, relating to payroll or administration)

Updated: November 2017 by S.Allen & R.Mansoor To be reviewed by November 2018

### **Links to other Fyling Hall policies and documents**

A separate E-Safety policy exists <http://www.fylinghall.org/wp-content/uploads/2013/04/e-safety-policy.pdf>

A separate ICT Acceptable Use policy exists <http://www.fylinghall.org/wp-content/uploads/2013/04/ICT-Acceptable-Use-Policy-1.pdf>

Parental Guide to Keeping Children and Young People Safe On-line  
<http://www.fylinghall.org/wp-content/uploads/2013/04/Parents-guide-to-e-safety.pdf>

Privacy Notice is available on the Fyling Hall website <http://www.fylinghall.org/>

Staff Capability and Disciplinary Procedure

### **Useful websites and contacts:**

Data Protection Act (1998) <http://www.legislation.gov.uk/ukpga/1998/29/contents>

Education Act (1996) <http://www.legislation.gov.uk/ukpga/1996/56/section/576>

European Commission (data transfers outside the European Union)  
[http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm)

Information Commissioner's Office <https://ico.org.uk>

Fyling Hall School  
SUBJECT ACCESS REQUEST FORM – DATA PROTECTION ACT 1998

Enquirer's full name.....  
Address.....  
Postcode.....  
Telephone number.....  
Name of data subject.....

Are you the person who is the subject of the records you are enquiring about (the 'data subject')? YES / NO

If NO, are you a parent of the data subject as defined in the Education Act 1996? YES / NO

Two forms of identification (one photographic and one showing a current address) are required to verify your identity. Have these been included? YES / NO

Please provide a description of the information requested (for example, you may be requesting emails relating to a specific event or a copy of your whole personnel file)

**Declaration**

I request that Fyling Hall search its records based on the information supplied above under Section 7(1) of the Data Protection Act (1998).

I agree that the reply period will commence when I have supplied sufficient information to enable Fyling Hall to perform the search.

I consent to the reply being disclosed and sent to me at my stated address.

Signature of data subject / parent.....  
Please PRINT name .....  
Date.....

This form should be returned to:

Mr Steven Allen  
Fyling Hall School  
Robin Hood's Bay,  
North Yorkshire,  
England,  
YO22 4QD

### **Fees**

The following fees will apply to cover the administrative costs to Fyling Hall of fulfilling a request (an invoice will be sent to you once your request has been processed)

<b>Number of pages</b>	<b>Maximum fee</b>	<b>Number of pages</b>	<b>Maximum fee</b>
1-19	£1	100-149	£10
20-29	£2	150-199	£15
30-39	£3	200-249	£20
40-49	£4	250-299	£25
50-59	£5	300-349	£30
60-69	£6	350-399	£35
70-79	£7	400-449	£40
80-89	£8	450-499	£45
90-99	£9	500+	£50