Information and Data Protection Policy

(please note that any reference to GDPR may be subject to change as the Data Protection Bill progresses)

Introduction

This policy is to ensure that Fyling Hall School complies with the requirements of the General Data Protection Regulation (GDPR), Data Protection Act 2018, associated guidance and Codes of Practice issued under the legislation.

Scope

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.

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

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.

The Information and Data Protection Policy applies to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

Information Security and security incident reporting is addressed in the ICT Acceptable Use policy.

Data Protection

Personal data will be processed in accordance with the requirements of GDPR and in compliance with the data protection principles specified in the legislation.

The school has notified the Information Commissioner's Office that it is a Data Controller. 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.

Fyling Hall has appointed a Data Protection Officer (DPO). Details of the DPO can be found here:

Information Governance
Veritau Ltd
County Hall
Racecourse Lane
Northallerton
DL7 8AL

schoolsDPO@veritau.co.uk
01609 53 2526

The DPO is a statutory position and will operate in an advisory capacity. Duties will include:

- Acting as the point of contact for the Information Commissioner's Office (ICO) and data subjects;
- Facilitating a periodic review of the corporate information asset register and information governance policies;
- Assisting with the reporting and investigation of information security breaches
- Providing advice on all aspects of data protection as required, including information requests, information sharing and Data Protection Impact Assessments; and
- Reporting to the trustees on the above matters

Information Asset Register

The DPO will advise the school in developing and maintaining an Information Asset Register (IAR). The register will include the following information for each asset:

- An individual information asset identification number;
- The owner of that asset;
- Description and purpose of the asset;
- Whether there is a privacy notice published for that asset;
- Format and location of the asset;

- Which officers (job titles/teams) have routine access to the information;
- Whether there are any data sharing agreements relating to the information and the name of that agreement,
- Conditions of data processing;
- Details of any third parties contracted to process the information;
- Retention period for the asset

The IAR will be reviewed annually and the Head Teacher will inform the DPO of any significant changes to their information assets as soon as possible.

Information Asset Owners

An Information Asset Owner (IAO) is the individual responsible for an information asset, understands the value of that information and the potential risks associated with it. The school will ensure that IAOs are appointed based on sufficient seniority and level of responsibility.

IAOs are responsible for the security and maintenance of their information assets. This includes ensuring that other members of staff are using the information safely and responsibly. The role also includes determining the retention period for the asset, and when destroyed, ensuring this is done so securely.

Training

The school will ensure that appropriate guidance and training is given to the relevant staff, trustees and other authorised school users on access to information procedures, records management and data breach procedures. Individuals will also be made aware and given training in relation to information security including using email and the internet.

The DPO will be consulted in relation to training where necessary; to ensure training resources and their implementation are effective.

The school will ensure that any third party contractors have adequately trained their staff in information governance by carrying out the appropriate due diligence.

Privacy notices

Fyling Hall School will provide a privacy notice to data subjects each time it obtains personal information from or about that data subject. Our main privacy notice will be displayed on the school's website in an easily accessible area. This notice will also be provided in a hard copy to pupils and parents at the start of the year as part of their information pack. A privacy notice for employees will be provided at commencement of their employment with the school. Specific privacy notices will be issued where the data subject requires more information about specific processing (e.g. school trips, projects).

Privacy notices will be cleared by the DPO prior to being published or issued. A record of privacy notices shall be kept on the school's Information Asset Register.

Information sharing

In order to efficiently fulfil our duty of education provision it is sometimes necessary for the school to share information with third parties. Routine and regular information sharing arrangements will be documented in our main privacy notice (as above). Any ad hoc sharing of information will be done in compliance with our legislative requirements.

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 1998. 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 permittedto 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

There may be instances where we are required to disclose personal data without the consent of the data subject. This includes where we have a legal obligation to do so for crime or taxation purposes. Any disclosures made in this instance will be in accordance with Schedule 2(2) of the Data Protection Act 2018.

Data Protection Impact Assessments (DPIAs)

The school will conduct a data protection impact assessment for all new projects involving high risk data processing as defined by GDPR. This assessment will consider the privacy risks and implications of new projects as well as providing solutions to the identified risks

The DPO will be consulted at the start of a project and will advise whether a DPIA is required. If it is agreed that a DPIA will be necessary, then the DPO will assist with the completion of the assessment, providing relevant advice.

Retention periods

Retention periods will be determined by any legal requirement, best practice or national guidance, and lastly the organisational necessity to retain the information. In addition IAOs will take into account the Limitation Act 1980, which provides timescales within which action may be taken for breaches of the law, when determining retention periods.

Destruction of records

Retention periods for records are recorded in the school's IAR. When a record reaches the end of its retention period the IAO will arrange for the records, both electronic and paper to be destroyed securely. Provisions to destroy paper information securely include cross cutting shredders and confidential waste bins. Advice in regards to the secure destruction of electronic media will be sought from relevant IT support.

A record should be retained of all files destroyed including, where relevant:

- File reference number,
- Description of file,
- Date of disposal,
- Method of disposal,
- Officer who destroyed record

Third party Data Processors

All third party contractors who process data on behalf of the school must be able to provide assurances that they have adequate data protection controls in place to ensure that the data they process is afforded the appropriate safeguards. Where personal data is being processed, there will be a written contract in place with the necessary data protection clauses contained.

Relevant senior leadership may insist that any data processing by a third party ceases immediately if it believes that that third party has not got adequate data protection safeguards in place. If any data processing is going to take place outside of the EEA then the Data Protection Officer must be consulted prior to any contracts being agreed.

Access to information

Requests for information under the GDPR- Subject Access Requests

Requests under this legislation should be made to the head teacher

Any member of staff/trustee may receive a request for an individual's personal information. Whilst GDPR does not require such requests to be made in writing, applicants are encouraged where possible to do so; applicants who require assistance should seek help from the school. Requests will be logged with the school office and acknowledged within 5 days.

We must be satisfied as to your identity and may have to ask for additional information such as:

- Valid Photo ID (driver's licence, passport etc);
- Proof of Address (Utility bill, council tax letter etc);
- further information for the school to be satisfied of the applicant's identity;

Only once the school is satisfied of the requestor's identity and has sufficient information on which to respond to the request will it be considered valid. We will then respond to your request within the statutory timescale of 30 **calendar** days.

The school can apply a discretionary extension of up to 60 calendar days to comply with the request if the requested information would take a considerable amount of time to collate, redact, and prepare for disclosure due to either the complexity or voluminous nature of the records. If we wish to apply an extension we will firstly seek guidance from our DPO, then inform the applicant of the extension within the first 30 days of receiving the request. This extension period will be kept to a minimum and will not be used as a way of managing workloads. In very limited cases we may also refuse a request outright as 'manifestly unreasonable' if we would have to spend an unjustified amount of time and resources to comply.

Should we think any exemptions are necessary to apply we will seek guidance from our DPO to discuss their application.

If a subject access request is made by a parent whose child is 12 years of age or over we may consult with the child or ask that they submit the request on their own behalf. This decision will be made based on the capacity and maturity of the pupil in question.

Requests received from parents asking for information held within the pupil's Education Record will be dealt with under the Education (Pupil Information)(England) Regulations 2005. Any charges which arise from this request will be applied at our discretion.

Data Subject rights

As well as a right of access to information, data subjects have a series of other rights prescribed by the GDPR including:

- Right to rectification
- Right to erasure
- Right to restrict processing
- Rights in relation automated decision making and profiling

All requests exercising these rights must be in writing and forwarded to the head teacher who will acknowledge the request and respond within 30 calendar days. Advice regarding such requests will be sought from our DPO. Please note that these rights are not automatic and may be subject to certain exemptions within the Act.

A record of decisions made in respect of the request will be retained, recording details of the request, whether any information has been changed, and the reasoning for the decision made.

Complaints

Complaints in relation to Subject Access will be handled through our existing procedures. Any individual who wishes to make a complaint about the way we have handled their personal data should contact the DPO on the address provided.

Copyright

Fyling Hall School will take reasonable steps to inform enquirers if any third party might have a copyright or intellectual property interest in information provided in response to their requests. However it will be the enquirer's responsibility to ensure that any information provided by the school is not re-used in a way which infringes those interests, whether or not any such warning has been given.

General

The Trustee Board will be responsible for evaluating and reviewing this policy.

Signed: **Date:**

Review Date:

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

Fyling Hall School
SUBJECT ACCESS REQUEST FORM – DATA PROTECTION ACT 2018

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 in accordance with Article 15 of the General Data Protection Legislation.
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