Policy title	**Data Protection Policy (GDPR-compliant)/Freedom of Information (GDPR – complaint)**
Date policy ratified by Governing Body	
Signed by **Print name**	
Effective date	**May 2018** **(updated 03.12.18)**
Review frequency	**Annually**
Review date	**March 2019**
Governing Body Sub-Committee	**Steering Group**

The Hayfield School
Hurst Lane
Auckley
Doncaster
DN9 3HG

Telephone 01302 770589

Data Protection Policy (GDPR-compliant)

Introduction

The Hayfield School collects and uses certain types of personal information about staff, students, parents and other individuals who come into contact with the school, in order to provide education and associated functions. The school may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and in accordance with the General Data Protection Regulation (GDPR) and other related legislation.

The GDPR applies to all computerised data and manual files if they come within the definition of a "filing system" ie where the data is structured in some way that is searchable on the basis of specific criteria, such as by an individual's name, regardless of where the data is located and how it is held (manual or electronic).

This policy will be updated as necessary to reflect best practice, or when amendments are made to Data Protection Legislation.

Personal Data

"Personal Data" is any information that identifies an individual, and includes information which would identify an individual to the person to whom it is disclosed because of any other knowledge that they already have or can obtain. A sub-set of Personal Data is "Special Category Personal Data", which relates to:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trades union membership
- Physical or mental health
- An individual's sex life or sexual orientation
- Generic or biometric data for the purpose of uniquely identifying a natural person

"Special Category Personal Data" is given specific additional protection under GDPR and additional safeguards apply as to how this information is collected, stored and used.

Information relating to criminal convictions will only be held and processed where there is legal authority to do so.

The Hayfield School does not intend to seek or hold sensitive personal data about staff or students except where the school has been notified of the information, or it comes to the school's attention via legitimate means eg a grievance or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff and students are under no obligation to disclose to the school their race or ethnic origin, political or religious beliefs, whether or not they are a Trades Union member or details of their sexual life (except

to the extent that details of marital status and/or parenthood are required for other purposes eg pension entitlements).

Data Protection Principles

The Hayfield School follows at all times the six data protection principles established under GDPR as follows:

- Personal data shall be processed fairly, lawfully and in a transparent manner and processing shall not be lawful unless one of the processing conditions is met;
- Personal data shall be collected for specific, explicit, legitimate purposes and shall not be further processed in a manner incompatible with those purposes;
- Personal data shall be adequate, relevant and limited to that which is necessary for the purposes for which it is being processed;
- Personal data shall be accurate and where necessary kept up to date;
- Personal data processed for any purposes shall not be kept for longer than is necessary for those purposes;
- Personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

In addition, the school is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law, as explained later in this policy.

The Hayfield School will at all times:

- Inform individuals as to the purpose of collecting any information from them, as and when we request the information;
- Be responsible for checking the quality and accuracy of that information;
- Regularly review the records held to ensure that information is not held longer than is necessary and that it has been held in accordance with the school's **Records Management Policy**;
- Ensure that when information is authorised for disposal it is done appropriately;
- Ensure appropriate security measures to safeguard personal data whether it is held in paper files or on a computer system and follow the relevant security requirements at all times;
- Share personal data with others only when it is necessary and legally appropriate to do so
- Set out clear procedures for responding to requests for access to personal data (known as **Data Subject Access Requests**);
- Report any breaches of GDPR in accordance with the procedures set out later in this Policy.

Conditions for processing in the first Data Protection Principle

- The individual has given consent that is specific to the particular type of processing activity and that consent is informed, unambiguous and freely given;

- The processing is necessary for the performance of a contract to which the individual is a party, or is necessary for the purpose of taking steps with regard to entering into a contract with the individual, at their request;
- The processing is necessary for the performance of a legal obligation to which the school is subject;
- The processing is necessary to protect the vital interests of the individual or another;
- The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the school;
- The processing is necessary for a legitimate interest of the school or that of a third party, except where this interest is over-ridden by the rights and freedoms of the individual concerned.

Use of Personal Data by The Hayfield School

The Hayfield School holds personal data on staff, students and other individuals such as visitors. In each case, the personal data must be treated in accordance with the Data Protection Principles outlined above.

Students

The personal data held regarding students includes contact details, assessment/examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information and photographs.

This data is used in order to support the education of students, to monitor and report on their progress, to provide appropriate pastoral care and to assess the performance of the school overall, together with any other uses normally associated with this provision in a school environment.

In the course of this legitimate and limited processing activity, the school may:

- Transfer information to any association, society or club set up for the purpose of maintaining contact with former students or for fundraising, marketing or promotional purposes relating to the school, but only where consent has been obtained first;
- Make personal data, including Special Category Personal Data, available to staff for planning curricular and extra-curricular activities;
- Keep the student's previous school informed of his/her academic progress and achievements during the student's first year at The Hayfield School;
- Use photographs of students in accordance with the school's **Admissions Policy**.

If parents or carers wish to object to or limit any use of personal data they should notify the Headteacher in writing, which notice will be acknowledged in writing. If, in the view of the Headteacher, the objection cannot be sustained, the parent or carer will be given written reasons why the school cannot comply with their request.

Biometric Recognition Systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use fingerprints/thumbprints to receive school dinners instead of

paying with cash), we comply with the requirements of the Protection of Freedoms Act 2012, under which a “child” means any person under 18 years old.

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

Parents/Carers and students have the right to choose not to use the school’s biometric system. We will provide alternative means of accessing the relevant services for those students, such as a PIN Code, for example.

Parents/Carers and students can object to participation in the school’s biometric system, or withdraw consent, at any time, and we will make sure that any relevant data already captured is securely deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student’s parents/carers.

Where staff members, or other adults, use the school’s biometric system, we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will securely delete any relevant data already captured.

Staff

The personal data held about staff will include contact details, employment history, information related to career progression, information related to DBS checking and photographs.

This data is used to comply with legal obligations placed on the school in relation to employment and the education of children in a school environment. The school may pass information on to other regulatory authorities where appropriate. Personal data will also be used when giving references.

Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as “spent” once the period of sanction has expired, the details of the incident may need to be kept for a longer period (see **Records Management Policy**).

Any wish to limit or object to the uses to which personal data is to be put should be notified to the Human Resources Manager who will ensure that this is recorded and adhered-to if appropriate. If the Human Resources Manager is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why the school cannot comply with their request.

Other Individuals

The Hayfield School may hold personal data in relation to other individuals who come into contact with the school. This may include, but is not restricted to, contractors, visitors and

guests. Such personal data shall be held only in accordance with the Data Protection Principles outlined above and shall not be kept for longer than necessary.

CCTV

The Hayfield School uses CCTV in various locations around the school site to ensure it remains safe. We adhere to the ICO's Code of Practice for the Use of CCTV in Schools.

Whilst we do not need to obtain individuals' permission to use CCTV on our premises, we do make it clear where people's images are being recorded. **Security cameras are clearly visible and accompanied by prominent signs at public entrances to the building, explaining that CCTV is in use and providing contact details for the system**.

We do not record audio through the CCTV system. For further information, please see our **CCTV Policy**.

Security of Personal Data

The Hayfield School will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this policy and their duties under GDPR. The school will take all reasonable steps to ensure that all personal data is held securely and is not accessible to unauthorised persons.

Security of the school's ICT systems is of paramount importance and it is essential that staff do not jeopardise this by their actions. See the E-Safety Policy and ICT and Use of Internet Staff Policy for further details. Any deliberate attempt by a member of staff to circumvent the school's ICT security would be regarded as a serious disciplinary offence.

Disclosure of Personal Data to Third Parties

The Hayfield School will, in the normal course of its business, authorise disclosure of relevant personal data to third parties in the following circumstances:

- To give a confidential reference to a current or former employee, volunteer or student;
- For the prevention or detection of crime;
- For the assessment of any tax or duty payable;
- Where it is necessary to exercise a right or obligation conferred or imposed by law upon the school (other than an obligation imposed by contract);
- For the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
- For the purpose of obtaining legal advice;
- For research, historical and statistical purposes, so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress;
- To publish the results of public examinations or other achievements of students of the school;

- To disclose details of a student's medical condition where it is in the student's interests to do so eg for medical advice, insurance purposes or to organisers of school trips;
- To provide information to another educational establishment to which a student is transferring;
- To provide information to the Examinations Authority as part of the examination process;
- To provide information to the relevant Government Department concerned with national education. At the present time this is the Department for Education (DfE). The Examinations Authority may also pass information to the DfE.

The DfE uses information about students for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or Agencies strictly for statistical or research purposes.

The school may receive requests from third parties (ie those other than the individual, the school and employees of the school) to disclose personal data it holds about students, their parents or carers, staff and other individuals. This information will not generally be disclosed unless one of the specific exemptions under Data Protection legislation which allow such disclosure applies; or where necessary for the legitimate interests of the individual concerned or the school.

All such requests for the disclosure of personal data must be sent to the Headteacher in writing, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of the third party before making any disclosure.

Confidentiality of Student concerns

Where a student seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parent or carer, the school will maintain confidentiality unless it has reasonable grounds to believe that the student does not fully understand the consequences of withholding their consent, or where the school believes disclosure will be in the best interests of the student or other students.

Anybody who makes a request to see any personal information held about them by the school is making a data Subject Access Request. All information relating to the individual, including that held in manual or electronic files, should be considered for disclosure, provided that they constitute a "filing system" (see above for definition).

All such requests must be addressed to the Headteacher in writing and must be dealt with preferably on receipt and at the latest within one calendar month of receipt.

Where a child or young person does not have sufficient understanding to make their own request (usually those under the age of 12, or over 12 but with special educational needs which makes understanding of their information rights more difficult), a person with parental responsibility can make a request on their behalf. However, the Headteacher must be satisfied that (a) the child or young person lacks sufficient understanding and (b) the request made on their behalf is in their interests.

Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances, the school must have written evidence that the individual has authorised the person to make the application and the Headteacher must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

Access to records will be refused in instances where an exemption applies eg information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

A Data Subject Access Request must be made in writing. The school may ask for any further information reasonably required to locate the data being requested.

An individual only has the right of access to information about themselves and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

All records must be reviewed by the Headteacher before any disclosure takes place. Access to data will not be granted before this review has been completed.

Where all the data in a document cannot be disclosed, a permanent copy should be made and the data obscured or re-typed if this is more appropriate. Copies of the full original and altered documents should be retained, along with a note as to the reason why the document was altered.

Exemptions of access to Data by Subjects

Where a claim to legal professional privilege could be maintained in legal proceedings, the data is likely to be exempt from disclosure unless the privilege is waived.

There are other exemptions from the right of Subject Access. If the school needs to apply any of them to a specific request, the school will usually explain which exemption is being applied and why.

Other rights of individuals

The Hayfield School has an obligation to comply with the rights of individuals under the law and takes these rights seriously.

Right to object to Processing

- An individual has the right to object to the processing of their personal data on the grounds of pursuit of public interest or legitimate interest (see above) where they do not believe that those grounds are made out.
- Where such an objection is made, it must be sent to the Headteacher within two working days of receipt by the school and the Headteacher will assess whether there are compelling legitimate grounds to continue processing which over-ride the

interests, rights and freedoms of the individual(s), or whether the data is required for the establishment, exercise or defence of legal proceedings.

- The Headteacher will then be responsible for notifying the individual of the outcome of their assessment within five working days of receipt of the objection.

Right to Rectification

- An individual has the right to request rectification of inaccurate data without undue delay. Where any request for rectification is received, it must be sent to the Headteacher within two working days of receipt by the school and where adequate proof of inaccuracy is provided, the data shall be amended as soon as reasonably practicable and the individual duly notified that this has happened.
- Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data and communicated to the individual. The individual shall be given the option of a review under the complaints procedure or an appeal direct to the Information Commissioner.
- An individual also has a right to have incomplete information completed by providing the missing data and any information submitted in this way shall be updated without delay.

Right to Erasure

Individuals have the right, in certain circumstances, to have data permanently erased without undue delay.

- Where the personal data is no longer necessary for the purpose or purposes for which it was originally collected and processed;
- Where consent is withdrawn and there is no other legal basis for the processing;
- An objection has been raised under the right to object and is found to be legitimate;
- Personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);
- Where there is a legal obligation on the school to delete the data.

The Headteacher will make a decision regarding any application for erasure of personal data and will balance this request against the exemptions provided for in law. Where a decision is made to erase the data, and this data has been passed to other data controllers and/or has been made public, reasonable attempts to inform those controllers of the request shall be made.

Right to Restrict Processing

The processing of an individual's personal data may be restricted:

- Where the accuracy of the data has been contested, during the period when the school is attempting to verify the accuracy of the data;
- Where processing has been found to be unlawful and the individual has asked that there be a restriction on processing rather than erasure;

- Where data would normally be deleted, but the individual has requested that their information be kept for the purposes of the establishment, exercise or defence of a legal claim;
- Where there has been an objection made in relation to a Data Subject Access Request, pending the outcome of that decision.

Breaches of any requirements of GDPR

Any breach (or suspected breach) of any aspect of the provisions of GDPR shall be notified to the Headteacher immediately.

Once notified, the Headteacher shall assess:

- The extent of any actual breach
- The risks to the data subjects as a consequence of the breach
- Any security measures in place which will protect the data
- Any measures which can be taken immediately to mitigate the risk to individuals

Unless the Headteacher concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the school, unless a delay can be justified.

The Information Commissioner shall be told:

- Details of the breach, including the volume of data at risk and the number and categories of data subjects;
- The contact point for any enquiries (which would usually be the Headteacher);
- The likely consequences of the breach;
- Measures proposed or already taken to address the breach.

If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Headteacher shall notify the Data Subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

Data Subjects shall be told:

- The nature of the breach
- Who to contact with any questions
- Measures taken to mitigate any risks

The Headteacher shall then be responsible for instigating an investigation into the breach, including how it happened and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by a member of the Senior Leadership Team (or Governors if appropriate to the seriousness of the breach) and a decision made about the implementation of those recommendations.

Contact

The person legally responsible for GDPR in school is the Headteacher, who may delegate the operational aspects on a day-to-day basis to a senior member of the school staff.

Freedom of Information (FOIA) Policy (GDPR-compliant)

Purpose:

The Hayfield School is subject to the Freedom Of Information Act 2000 (FOIA) as a public authority and as such must comply with any requests for information in accordance with the principles laid out in the Act. Whilst The Hayfield School will not charge any Management or Handling Fees for responding to FOIA requests, we can and will charge for disbursements such as excessive photocopying or postage, although in reality most requests can be sent electronically and are therefore free of charge.

What constitutes an FOIA Request?

Any request for information from the school is technically a request under FOIA, whether or not the individual making the request mentions FOIA. However, the Information Commissioner's Office (ICO) has stated that routine requests for information (such as a parent requesting a further copy of a child's report) can be dealt with outside the provisions of the Act.

In all non-routine cases, if the request is simple and the information is to be released, then the member of staff who received the request can release the information, but must ensure that this is done within the timescale set out below. A copy of the request and the response should then be sent to the Headteacher.

All other requests should in the first instance be referred to the Headteacher who may allocate an appropriate member of staff to deal with the request. This must be done promptly and in any event within 3 working days of the school receiving the request.

When considering a request under FOIA, bear in mind that a release under FOIA is legally a release to the general public ie once it has been released to an individual, anyone can then access it and therefore attempts cannot be made to restrict access to information released under FOIA requests by marking it "Confidential" or "Restricted" or some such.

Time limit for Compliance

The school must respond as soon as possible and in any event within 20 working days of the date of receipt of the request. For schools, a "working day" is one on which students are in attendance. The absolute maximum is 60 calendar days in which the school must respond.

Procedure for dealing with a FOIA Request

When a request is received that cannot be dealt with by simply providing the information eg a school policy or holiday dates, it should be referred in the first instance to the Headteacher who may allocate a member of staff who has responsibility for the type of information requested.

The first stage in such a response is to determine whether or not the school "holds" the information requested. The school will "hold" the information if it exists in a computer or paper format. Some requests will require the school to take information from different sources and manipulate it in some way. Where this would take minimal effort, the school is considered to "hold" that information. However, if the required manipulation would take a significant amount of time, the individual making the request should be contacted to explain that the information is not held in the manner requested and offered the opportunity to refine their request.

For example, if the request required the school to add up totals on a spreadsheet and release the total figures, this would constitute information "held" by the school. Whereas if the school would have to go through a number of spreadsheets and identify individual figures to provide and release a total, this can be argued that it is not "held" by the school, dependent on the time required to extract and process the information.

Requests for information which is already publicly available or which can be easily extrapolated from that which is publicly available eg from a school's website, could also be refused on this basis.

The second stage is to decide whether the information can be released, or whether one of the exemptions set out in the FOI Act applies to all or part of the information requested. Common exemptions which might apply to information held by schools include, but are not limited to:

- Section 40 (1) – the request is for the applicant's personal data. This must be dealt with under the Data Subject Access Request regime under GDPR, detailed above;
- Section 40 (2) – compliance with the request would involve releasing third party personal data and this would be in breach of the GDPR principles detailed above;
- Section 41 – information which has been provided to the school (but not originated by the school) which is confidential;
- Section 21 – information which is already publicly available, even if payment of a fee is required to access that information;
- Section 22 – information that the school intends to publish at a future date in the normal course of its activities;
- Section 43 – information that would prejudice the commercial interests of the school and/or a third party;
- Section 38 – information that could prejudice the physical health, mental health or safety of an individual (this may apply especially to safeguarding issues);
- Section 31 – information which may prejudice the effective detection and prevention of crime eg a request for locations of CCTV cameras;
- Section 36 – information which, in the opinion of the Chair of Governors of the school would prejudice the effective conduct of the school. There is a special form for this on the ICO website to assist with obtaining the Chair's opinion.

Exemptions in some sections of FOIA are known as Qualified Exemptions. A Qualified Exemption requires the carrying out of a public interest weighting exercise, balancing the public interest in the information being released as against the public interest in withholding the information.

Responding to a Request

When responding to a request where the school has withheld some or all of the information, the school must explain why the information has been withheld, quoting the appropriate section number of FOIA and explaining how the requested information fits within that exemption. If the public interest test has been applied, this also needs to be explained.

The response should end by explaining to the requestor how they can complain – either by reference to an internal review by Governors or by contacting the ICO.

Contact

The person legally responsible for FOIA in school is the Headteacher, who may delegate the operational aspects on a day-to-day basis to a senior member of the school staff.