HAWTHORNS
SCHOOL

Individual Rights & Complaints Policy

Document Control Information			
Individual Rights and Complaints Policy, Issue 1 - May 2018			
Review Period Every 2 years		**Review Committee** Trustees	
Revision History			
Author	**Summary of changes**	**Issue**	**Date Authorised**
R Righini	Policy review re new GDPR rules	1	31st May 2018
Authorisation			
Approved By:	**This policy was approved by the Trustees.**		
Date Approved:	**31st May 2018**		
Date of Next review:	**31st May 2020**		
Document Owner & Reviewer:	The senior manager responsible for this policy is the Operations Director		
Equality Impact			
Statement	**We welcome feedback on this document and the way it operates. We are interested to know of any possible or actual adverse impact that may affect any groups in respect of any of the Equality Act 2010 protected characteristics.** **The person responsible for equality impact assessment for this document is the Director of Equality and Diversity.**		
Screening	**This document has been screened by the Equality Team and the impact has been assessed as:** ☐ **Not applicable** ☐ **Low** ☐ **Medium** ☐ **High**		

1. Purpose

1.1. We recognise the need for legal compliance and accountability and endorse the importance of the rights of data subjects and the requirement to provide a complaints mechanism.

1.2. This policy sets out the key requirements in relation to the exercise of individual rights and complaints to which we are fully committed

2. Scope of Policy

2.1. In order to fulfil its statutory and operational obligations we have to collect, use, receive and share personal, special personal and crime personal data about living people, eg,

2.1.1. Pupils and their families
2.1.2. current, past, prospective employees
2.1.3. clients and customers
2.1.4. contractors and suppliers
2.1.5. Governors members of the public (adults & children)

2.2. This policy covers the obligations to respond to individual rights and complaints in relation to personal data, regardless of data age, format, systems and processes purchased, developed and managed by/or on behalf of us and any person directly employed or otherwise by us.

2.3. This policy reflects the commitment to data protection compliance to both UK and EU legislation, in particular the Data Protection Act 2018, the EU General Data Protection Regulation 2016 (GDPR) and the EU Law Enforcement Directive 2016 (LED).

3. Reason for Review

3.1. This policy was reviewed in line with new GDPR regulations 2018.

4. Aim(s)

4.1. We aim for all stakeholders to have an informed knowledge of the rights of individuals with regards to their data. In addition, we aim for all data users to be sufficiently informed.

5. Policy

5.1. Data Protection Officer (DPO): We will appoint a data protection officer who will be the key contact for the provision of independent advice on all things data protection. The DPO will provide advice and support when dealing data subject enquiries and communications with the Information Commissioners Office.

Data Protection Officer
Barbara Mulvihill
Data Protection Officer on behalf of Hawthorns School.
West Street
Oldham
OL1 1UT

Email: DPO@oldham.gov.uk
Tel: 0161 770 1311

5.2 Individual Rights: Data subjects have the following rights: (see Appendix 1 for more information and the guide to individual rights:

5.2.1 The right to be informed
5.2.2 The right of access

5.2.3 The right to rectification
5.2.4 The right to erasure
5.2.5 The right to restrict processing
5.2.6 The right to data portability
5.2.7 The right to object
5.2.8 Rights in relation to automated decision making and profiling
5.2.9 The right to be informed in the event of a data security incident that poses a high risk

5.3 Plus data subjects are also able to:
5.3.1 seek a review/complain to the DPO
5.3.2 complain to the Information Commissioners Office (ICO)
5.3.3 seek judicial remedy, including compensation through the courts

These requests may be made verbally or in writing.

5.4 If a request is made verbally and the applicant refuses or is unable to put it in writing, it would be good practice provide the applicant with a written summary of your understanding of the request and ask them to confirm the summary is correct.

5.5 In all cases where there is any doubt as to the requestor's identity two proofs of identification will be necessary to confirm the requestor is who they say they are.

5.6 Where a request is 'manifestly unfounded, excessive or repetitious' the law says we can either:
5.6.1 Charge a fee to respond or
5.6.2 Refuse the request on one or more of these grounds

5.7 As a matter of policy, where we determine a request is manifestly unfounded, excessive of repetitious we intend to refuse the request. Where we refuse a request the onus rests on us to demonstrate that the request falls within the threshold for relying on one or more of these grounds.

5.8 Timescales for Response to individual rights requests and complaints: We will provide a written response within one calendar month* that explains the outcome of our decision with regards to an individual query/request and/or complaint.

5.9 The time starts the first day after receipt of the enquiry where we are satisfied with verification of the data subject's identity**.

5.10 This time can be extended to 2 calendar months where the case is complex or voluminous and the data subject has been informed of this within one calendar month of the original enquiry.

5.11 In the event of a serious data breach, we have an obligation to inform the data subject without undue delay if this poses a high risk for their privacy risks. This could mean that is some cases, the data subject is entitled to know before the 72 hour deadline for notifying the ICO.

5.12 *Note: the response needs to be within 21 days where the request is in relation to objection to processing, and in the event of a serious data breach, as soon as possible

5.13 **Note: and information to locate the personal data where the request is in relation to data subject access or objection to processing.

5.14 Reasons for lapsing requests: If ID and necessary information to locate requested information or to clarify what the requestor is asking, is not received then it may be necessary to 'lapse' the request if this is not received after 3 months.

5.15 Reasons for refusing requests: In addition to requests which may be considered manifestly unfounded and excessive requests etc, as outlined in 5.2, there are other likely exemptions that allow us to partially or wholly comply with individual rights. These are:

- 5.15.1 Rights of other individuals
- 5.15.2 Crime and taxation
- 5.15.3 Immigration
- 5.15.4 Determined by law, and legal proceedings
- 5.15.5 Public protection and regulatory functions
- 5.15.6 Parliamentary privilege
- 5.15.7 Judicial appointments/proceedings
- 5.15.8 Other people's data unless consent, or reasonable without consent
- 5.15.9 Self incrimination
- 5.15.10 Corporate finance
- 5.15.11 Management forecasts
- 5.15.12 Negotiations
- 5.15.13 Confidential references
- 5.15.14 Exams
- 5.15.15 Special purposes eg, artistic, literary, journalistic
- 5.15.16 Research and statistics
- 5.15.17 Archiving in the public interest

5.16 If the personal data is in relation to law enforcement, the exemptions include:

- 5.16.1 Prejudice/obstruction to prevention, detection, investigation, prosecution of crime
- 5.16.2 In the interests of public and national security and rights and freedoms of individuals, eg, privacy

5.17 The response to the data subject: The response to the data subject needs to contain the following:

- 5.17.1 Acknowledgement of the request/enquiry made
- 5.17.2 Whether or not we are able to comply with what the requestor is seeking, and an explanation of the reasons why not.
- 5.17.3 If we are unable to comply with what the request is seeking, and an explanation of the reasons why.
- 5.17.4 The right to complain to the ICO

5.18 Complaints: Please refer to our Compliments and Complaints policy

6 Assessment and Monitoring

6.2 An assessment of compliance with requirements will be undertaken in order to provide:

- 6.2.1 Assurance
- 6.2.2 Gap analysis of policy and practice
- 6.2.3 Examples of best practice
- 6.2.4 Improvement and training plans
- 6.2.5

6.3 Reports will be submitted to the Senior Management Team and Audit Committee.

7 Responsibilities and Approvals

7.2 Governing Body:

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

7.3 Headteacher:

The Headteacher acts as the representative of the data controller on a day-to-day basis and is responsible for the approval of this policy

7.4 Data Protection Officer:

The data protection officer will be the key contact for the provision of independent advice on all things data protection. The DPO will provide advice and support when dealing data subject enquiries and communications with the Information Commissioners Office

7.5 Governors/Employees:

All Governors and staff, whether permanent, temporary or contracted, including students, contractors and volunteers are responsible for ensuring they are aware of the data protection legislation requirements and for ensuring they comply with these on a day to day basis. Where necessary advice, assistance and training should be sought. Any breach of this policy could result in disciplinary action or could constitute a criminal offence.

6. Sources and references

6.1. Data Protection Act

7. Other useful documents

7.1. Subject Access Request Policy
7.2. Freedom of Information Policy
7.3. Privacy Notice Policy
7.4. Equality Policy
7.5. Publication Scheme
7.6. Complaints Policy

8. Monitoring

8.1. This policy will be monitored through the MAT's accountability framework.