Data Protection Policy

Chilton Academy

Policy Date:	24.03.21
Next Review Date:	24.03.21 Reviewed 01.04.22
Version number:	1.0
Approved by the Full Governing Board on	March 2021

1.0 Introduction

1.1 The School/Academy's Data Protection Policy has been produced to ensure compliance with the Data Protection Act 2018 (the DPA 2018), the General Data Protection Regulation ('GDPR') and all associated legislation,

1.2 The DPA 2018 gives individuals rights over their personal data and protects individuals from the erroneous use of their personal data.

1.3 The School/Academy is registered with the Information Commissioner's Office as the Data Controller for the purposes of the personal data its processes about individuals.

2.0 Purpose

2.1 The Policy is a requirement of the DPA 2018 and the GDPR.

2.2 The Policy outlines the School/Academy's overall approach to its responsibilities and legal obligations as the 'Data Controller' under the DPA 2018 and the GDPR.

3.0 Scope

3.1 This Policy applies to all employees (including temporary, casual or agency staff), governors, contractors and consultants working for, or on behalf of, the School/Academy. It also applies to any service providers that we contract with who process personal information on behalf of the School/Academy.

3.2 The Policy also covers any staff and students who may be involved in research or other activity that requires them to process or have access to personal data, for instance as part of a research project or as part of professional practice activities. If this occurs, it is the responsibility of the relevant School/Academy to ensure the data is processed in accordance with the DPA 2018 and that students and staff are advised about their responsibilities.

4.0 Data covered by the Policy

4.1 A detailed description of this definition is available from the ICO, however briefly, personal data is information relating to an individual where the structure of the data allows the information to be accessed i.e. as part of a relevant filing system. This includes data held manually and electronically and data compiled, stored or otherwise processed by the School/Academy, or by a third party on its behalf.

4.2 Special category data is personal data consisting of information relating to:

- Racial or ethnic origin
- Political opinions, Religious beliefs or other beliefs of a similar nature
- Membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- Physical or mental health or condition
- Sexual life or sexual orientation
- Biometric data

5.0 The Six Data Protection Principles

5.1 The DPA 2018 requires the School/Academy, including staff, governors and other individual who process personal information on behalf of the school, must comply with the six data protection principles.

5.2 The principles require that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- Be limited to only what is required for the purposes for which it is being collected
- Be accurate and kept up to date
- Not be kept for longer than is necessary for those purpose
- Be kept safe from unauthorised or unlawful processing and against accidental loss, destruction or damage

6.0 Responsibilities

6.1 The School/Academy has an appointed Data Protection Officer to.

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members

6. 2. The DPO reports to the highest level of management at the school, which is the Governing Body / Academy Trust

6.3. Our Data Protection Officer is provided by Mobile School Business Manager and can be contacted at the following address:

1 Abbey Road

Pity Me

Durham

DH1 5DQ

Info:mobile-sbm.com

6.4 All new members of staff will be required to complete a mandatory information governance module as part of their induction and existing staff will be requested to undertake refresher training on a regular / annual basis.

6.5 Employees of the School/Academy are expected to:

- Familiarise themselves and comply with the six data protection principles
- Ensure any possession of personal data is accurate and up to date
- Ensure their own personal information is accurate and up to date
- Keep personal data for no longer than is necessary
- Ensure that any personal data they process is secure and in compliance with the School/Academy's information related policies and strategies
- Acknowledge data subjects' rights (e.g. right of access to *all* their personal data held by the School/Academy) under the DPA 2018, and comply with access to records
- Ensure personal data is only used for those specified purposes and is not unlawfully used for any other business that does not concern the School/Academy
- Obtain consent with collecting, sharing or disclosing personal data
- Contact the DPO at info@mobile-sbm.com if they require advice or guidance, need to report data protection breach, or have any concerns relating to the processing of personal data under the DPA 2018.

6.4 Students, of the School/Academy are expected to:

- Comply with the six data protection principles
- Comply with any security procedures implemented by the School/Academy.

7.0 Obtaining, Disclosing and Sharing

7.1 Only personal data that is necessary for a specific School/Academy related business reason should be obtained.

7.2 Students are informed about how their data will be processed when they agree to the Data Processing Consent Notice upon registration.

7.3 Upon acceptance of employment at the School/Academy, members of staff also consent to the processing and storage of their data.

7.4 Data must be collected and stored in a secure manner.

7.5 Personal information must not be disclosed to a third-party organisation without prior consent of the individual concerned unless the disclosure is legally required or permitted. This also includes information that would confirm whether or not an individual is or has been an applicant, student or employee of the School/Academy.

7.6 The School/Academy may have a duty to disclose personal information in order to comply with legal or statutory obligation. The DPA 2018 may permit the school to share data without consent or without informing individuals in accordance with the Right to be Informed:

1. With the police and law enforcement bodies where it is considered necessary for the prevention and detection of crime;
2. Where the information may be necessary under enactment, for the purposes of legal proceedings and or for exercising of defending legal rights; and
3. Where the processing is necessary because it is a task carried out for in the public interest, for example, sharing information with the local authority, for example Safeguarding and Child Protection.

7.7 All requests from third party organisations seeking access, to personal data held by the school should be directed to the Headteacher and the Data Protection Officer at **info@mobile-sbm.com**. The School will keep a record of all requests received from third party organisations. This information may be requested by the DPO or the Information Commissioner at any time to comply and actively evidence compliance, with Data Subjects Rights.

7.8 Personal information that is shared with third parties on a more regular basis shall be carried out under written agreement to stipulate the purview and boundaries of sharing. For circumstances where personal information would need to be shared in the case of ad hoc arrangements, sharing shall be undertaken in compliance with the DPA 2018.

8.0 Retention, Security and Disposal

8.1 Recipients responsible for the processing and management of personal data need to ensure that the data is accurate and up-to-date. If an employee, student or applicant is dissatisfied with the accuracy of their personal data, then they must inform Mrs Dodsworth, Headteacher.

8.2 Personal information held in paper and electronic format shall not be retained for longer than is necessary. In accordance with Data protection Principles of the DPA 2018, personal information shall be collected and retained only for business, regulatory or legal purposes.

8.3 In accordance with the provisions of the DPA 2018, all staff whose work involves processing personal data, whether in electronic or paper format, must take personal responsibility for its secure storage and ensure appropriate measures are in place to prevent accidental loss or destruction of, or damage to, personal data.

8.4 In accordance with the School/Academy's Flexible Working Scheme, staff working from home will be responsible for ensuring that personal data is stored securely and is not accessible to others.

8.5 All departments should ensure that data is destroyed in accordance with the Retention Schedule when it is no longer required.

8.6 Personal data in paper format must be shredded or placed in the confidential waste bins provided. Personal data in electronic format should be deleted, and CDs and pen drives that hold personal data passed to your I.T provider for safe disposal. Hardware should be appropriately degaussed in compliance with your I.T service provider contract to ensure the data held on the external device is screened, reviewed before being degaussed and securely destroyed.

9.0 Transferring Personal Data

9.1 Any transfer of personal data must be done securely in line with the School/Academy's ICT / Computing policy and Acceptable User Agreements.

9.2 Email communication is not always secure and sending personal data via external email should be avoided unless it is encrypted with a password provided to the recipient by separate means such as via telephone.

9.3 Care should be taken to ensure emails containing personal data are not send to unintended recipients. It is important that emails are addressed correctly and care is taken when using reply all or forwarding or copying others in to emails. Use of the blind copy facility should be considered when sending an email to multiple recipients to avoid disclosing personal information to others.

9.4 Personal email accounts should not be used to send or receive personal data for work purpose.

10.0 Data Subjects (Subject Access Requests)

10.1 Under the DPA 2018, individuals (staff, pupils, parents and governors and students etc) have the following Rights:

- Access to personal information processed by the School/Academy;
- Object to processing of personal data that is likely to cause, or is causing, damage or distress
- Prevent processing for direct marketing
- Object to decisions being taken by automated means
- In certain circumstances, have inaccurate or incomplete personal data rectified, blocked, restricted, erased or destroyed.
- claim compensation for damages caused by a breach of the Data Protection regulations

10.2 Individuals can make a 'subject access request' to any member of school staff, verbally or in writing to request access to personal information the school holds about them, subject to any exemptions or restrictions that may apply.

10.3 The School/Academy shall use its discretion under the DPA 2018 to encourage informal access at a local level to a data subject's personal information, but the schools formal procedure for the processing of Subject Access Requests must be followed to comply with the DPA 2018.

10.4 Any individual who wishes to exercise their Right of Access can do so verbally or in writing. There is no legal requirement to ask the requester to keep the schools subject access request form, but it may ask the requester to do so. A copy of the Schools Subject Access Request form is available by contacting the Academy on 01388 720255.

10.5 The School/Academy may not charge fee. It will only release any information upon receipt of the completed Subject Access Request Form, along with proof of identity or proof of authorisation where requests are made on the behalf of a data subject by a third party. The requested information will be provided within the statutory timescale of 1 month from receipt of the completed form.

10.6 For details of your other rights, please see 'Your Information, Your Rights' booklet on our website at www.chilton.durham.sch.uk

11.0 Reporting a Data Security Breach

11.1 It is important the School/Academy responds to a data security breach quickly and effectively. A breach may arise from a theft, a deliberate attack on School/Academy systems, unauthorised use of personal data, accidental loss or equipment failure. Any data breach should be reported to the academy at chilton@durhamlaerning.net the Lead Investigation Officer will then inform the Data Protection Officer , and if it relates to an IT incident (including information security), should also be reported to the Headteacher and in certain circumstances to your I.T provider – please refer to the Data breach reporting policy for more information.

This policy applies to all staff and pupils and contractors at the school/academy. This includes teaching students, temporary, casual, agency staff, suppliers and data processors working for or on behalf of the school/academy.

11.2 Any breach will be investigated in line with the procedures within the Data Breach Policy. In accordance with that Policy, the School/Academy will treat any breach as a serious issue. Each incident will be investigated and judged on its individual circumstances and addressed accordingly.

11.3 If a breach occurs or is discovered outside normal working hours, it must be reported to school as soon as practicable. Note: the school/academy must report data breaches that result, or are likely to result, in high risk to the rights and freedoms of individuals to the Information Commissioner with undue delay and in any event within 72 hours.

11.4 The School will complete a Data Breach report that shall include the facts relating to the breach, its effect on individuals, the action taken by the school to mitigate any risks The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many people are involved.