



Teesside High School
Education as it should be

GDPR Compliant Data Protection Policy

DOCUMENT CONTROL	
Date Reviewed/Revised:	June 2018
Ratified by Governors:	20 June 2018
Date of next Review:	June 2019

F&GP

TEESSIDE HIGH SCHOOL

Policy Name	Data Protection Policy
Purpose	To ensure that data is dealt with appropriately, ethically, and in line with legislative requirements
Applies to	Students, parents, current and former employees, workers, volunteers, apprentices, contractors and consultants of the School and any subsidiary.
Other associated policies and documents	
Date reviewed and updated	May 2018

This policy supersedes the School's previous Data Protection Policy.

1 Introduction

- 1.1 Teesside High School ("The School") takes the security and privacy of personal data seriously and ensures that personal data is processed in a transparent and lawful manner.
- 1.2 The gathering and processing of data is a fundamental requirement of our business activity in order to maintain relationships with individuals. However, at all times we will comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') and the **EU General Data Protection Regulation** ('GDPR') in respect of data privacy and security. As part of our obligations and ongoing commitments to staff and other groups whose data we hold and process, we have a duty to openly communicate the information contained in this policy.
- 1.3 This policy applies to students, parents, current and former employees, workers, volunteers, apprentices, contractors and consultants of the School and any subsidiary. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services agreement) and any other documentation we issue to you from time to time in relation to personal data.
- 1.4 The School is a '**data controller**' for the purposes of personal data. This means that we determine the purpose and means of the processing of personal information.
- 1.5 This policy explains how the School will hold and process personal information and it explains individual rights as a 'data subject'. It also explains the obligations on all staff (permanent and temporary employees, workers, contractors and volunteers) when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of the School.

- 1.6 The School does have separate privacy statement and notices in place in respect of job applicants, employees, customers/clients, suppliers and other categories of data subject in addition to this policy, which will always communicate clearly, and will outline the reason for processing data, how the data will be processed, shared and stored. A copy of the School's privacy statement can be obtained on www.teessidehigh.co.uk.
- 1.7 This policy does not form part of your contract of employment, contract of admission or contract of services and can be amended by the School at any time. It is intended that this policy is fully compliant with the Act and the GDPR.

2 Data Protection Principles

- 2.1 Personal data must be processed in accordance with six '**Data Protection Principles.**'

It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

The School is accountable for these principles and must be able to show compliance with these principles at all times.

3 How we define personal data

- 3.1 '**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person, but it does not include anonymised data.
- 3.2 This policy applies to all personal data whether it is stored electronically, on paper or on other materials.
- 3.3 This personal data might be provided to the School, by staff, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by the School. It could also be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by a member of staff's direct manager or other colleagues.
- 3.4 The School will collect and use the following types of personal data about staff (employee's, workers and contractors) working for the School:
- recruitment information such as application forms and CV's, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
 - contact details and date of birth;

- the contact details of any emergency contacts;
- gender;
- marital status and family details;
- information about contracts of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
- bank details and information in relation to tax status including a national insurance number;
- identification documents including passport and driving licence, and information in relation to immigration status and right to work for us;
- information relating to disciplinary or grievance investigations and proceedings involving staff (whether or not you are the main subject of those proceedings);
- information relating to performance and behaviour at work;
- training records;
- electronic information in relation to use of IT systems/swipe cards/telephone systems;
- images (whether captured on CCTV, by photograph or video);
- information in relation to specific accreditation or recognition required to carry out workplace tasks; and
- any other category of personal data which we may notify you of from time to time.

4 How we define special categories of personal data

4.1 **'Special categories of personal data'** are types of personal data consisting of information as to:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic or biometric data;
- health;
- sex life and sexual orientation; and
- any criminal convictions and offences.

The School may hold and use any of these special categories of your personal data in accordance with the law.

5 How we define processing

5.1 **'Processing'** means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

6 How will we process your personal data?

6.1 The School will process personal data (including special categories of personal data) in accordance with our obligations under the GDPR.

6.2 In particular, personal data will be used:

- to perform the contract of employment (or services) between you and the School;
- in complying with any legal obligation; or
- if it is necessary for the School's legitimate interests (or for the legitimate interests of someone else). However, the School can only do this if the 'data subject's' interests and rights do not override that of the School (or that of someone else). The 'data subject' will also have the right to challenge the School's legitimate interests and request that it stop's this processing. See details of rights as a 'data subject' in section 12 below.

The School can process personal data for the above purposes without individual knowledge or consent but will not use personal data for an unrelated purpose without telling the 'data subject' about it, and the legal basis that the School intends to rely on for processing it.

If an individual chooses not to provide the School with certain personal data, it is important that they are aware that we may not be able to carry out certain parts of the contract between both parties. For example, if an employee does not provide the School with bank account details, the School may not be able to pay the employee. It might also stop the School from complying with certain legal obligations and duties, such as to pay the right amount of tax to HMRC.

7 When the School might process personal data

7.1 The School has to process personal data in various situations during recruitment, employment (or engagement) and even following termination of employment (or engagement).

7.2 For example (and see section 7.6 below for the meaning of the asterisks):

- to decide whether to employ (or engage) with a member of staff;
- to decide how much to pay a member of staff, and decide on other terms applicable to a contract;
- to check a legal right to work in the UK;
- to carry out the contract between parties, including where relevant, its termination;
- training and reviewing of performance*;
- to decide whether to promote a member of staff;
- to decide whether and how to manage performance, absence or conduct matters*;
- to carry out a disciplinary or grievance investigation or procedure in relation to an individual member of staff or someone else;
- to determine whether the School needs to make reasonable adjustments to the workplace or a role because of a disability*;
- to monitor diversity and equal opportunities*;
- to monitor and protect the security (including network security) of the School, of staff, of customers and others;

- to monitor and protect the health and safety of all staff, customers and third parties*;
 - to pay staff and provide pension and other benefits in accordance with a contract in place*;
 - paying tax and national insurance;
 - to provide a reference upon request from another employer;
 - to pay trade union subscriptions*;
 - monitoring compliance by staff, the School and others with our policies and contractual obligations*;
 - to comply with employment law, immigration law, health and safety law, tax law and other laws which affect the School*;
 - to answer questions from insurers in respect of any insurance policies which relate to individual members of staff*;
 - coordinating the School's business activity and planning for the future;
 - the monitoring, prevention and detection of fraud or other criminal offences;
 - to defend the School in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*;
 - for any other reason which the School may notify 'data subject's' of from time to time.
- 7.3 The School will only process special categories of personal data (see above) in certain situations in accordance with the law. For example, the School can do so if they have explicit consent from a 'data subject'.
- 7.4 If the School has asked for consent from a 'data subject' to process a special category of personal data, the reasons for this would be explained, and consent does not need to be given. If consent is given, it can be withdrawn at a later date by contacting the Finance Manager by sending an email to jpumphrey@teessidehigh.co.uk.
- 7.5 The School do not need your consent to process special categories of your personal data when processing it for the following purposes, which the School may do:
- where it is necessary for carrying out rights and obligations under employment law;
 - where it is necessary to protect a 'data subjects' vital interests or those of another person, where they are physically or legally incapable of giving consent;
 - where data is made public;
 - where processing is necessary for the establishment, exercise or defence of legal claims; and
 - where processing is necessary for the purposes of occupational medicine or for the assessment of an employees working capacity.
- 7.6 The School might process special categories of personal data for the purposes in paragraph 7.2 above which have an asterisk beside them. In particular, the School will use information in relation to:
- race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
 - sickness absence, health and medical conditions to monitor level of absences, assess fitness for work, to pay benefits, to comply with legal obligations under

employment law, including to make reasonable adjustments and to look after the health and safety of staff on site;

- trade union membership to pay any subscriptions and to comply with legal obligations in respect of trade union members; and
- DBS checks and the other relevant safeguarding and employment checks

7.7 The School will not make automated decisions based on personal data, or data profiling of 'data subjects' where a potentially damaging decision is taken without human intervention.

8 Sharing personal data

8.1 Sometimes the School might share personal data with group companies or contractors and agents to carry out obligations under a contract with a 'data subject' or to pursue the School's legitimate interests. For example, the School employ the services of a HR consultancy to provide advice and support in relation to HR and employment law. On occasion it will be necessary to share personal data with the third party HR consultancy School to seek advice in accordance with employment law legislation.

8.2 The School do require any third party to keep personal data confidential and secure and to protect the data in accordance with the law, and School policies. Third parties are only permitted to process data for the lawful purpose for which it has been shared and in accordance with the School's instructions.

8.3 The School does not send personal data outside of the European Economic Area. If this changes then any affected staff will be notified and measures to protect the security of such data will be explained.

9 How are staff (permanent and temporary employees, workers, contractors and volunteers) required to process personal data for the School?

9.1 Everyone who works for, or on behalf of the School has a responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and to ensure the School's rules on data security and retention are complied with.

9.2 Personnel files will be held indefinitely due to the possibility of future legal action or historic abuse claims, as recommended by the Independent Inquiry into Child Sexual Abuse.

9.3 CVs and interview notes are held for 12 months following an interview or application in order to comply with any legal or contractual obligations.

9.4 Student files will be held until they are 25 years old or in the case of SEN students 30 years old.

9.5 Parental financial data will be held of seven years after the student has left the school.

9.6 You should only access personal data covered by this policy if it is needed for the performance of your workplace duties, and only if you have the authorisation to do so by a line manager. On this point, it is important to note that personal data should only be used for the specified lawful purpose for which it was obtained.

9.7 Personal data must not be shared informally.

- 9.8 You have a responsibility to keep personal data secure and not share it with unauthorised people.
- 9.9 You are required to regularly review and update personal data which you have to deal with for work. This includes telling the School if your own personal details change.
- 9.10 You should not make unnecessary copies of personal data and you must dispose of any copies securely.
- 9.11 You are expected to use strong passwords for IT related systems.
- 9.12 You should lock your computer screens when not at your desk.
- 9.13 Personal data should be encrypted before being transferred electronically to authorised external contacts.
- 9.14 Do not save personal data to your own personal computers or other devices.
- 9.15 Personal data should never be transferred outside the European Economic Area except in compliance with the law and only with written authorisation from the Finance Manager.
- 9.16 You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.
- 9.17 You should not take personal data away from School's premises without authorisation from your line manager or the Head.
- 9.18 Personal data should be shredded and disposed of securely when you have finished with it.
- 9.19 You should ask for help from your line manager if you are unsure about data protection or if you notice any areas of data protection or security that the School can improve upon.
- 9.20 Any deliberate or negligent breach of this policy by you may result in disciplinary action in accordance with the School's disciplinary procedure, and it is important that you are aware that any such deliberate or negligent actions may amount to Gross Misconduct and could result in your dismissal. Other forms of remedial action can be taken where appropriate, such as is the case with contractors, workers and/or volunteers.
- 9.21 It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in dismissal.
- 9.22 The Finance Manager is responsible for reviewing this policy and updating the Board of Directors on the School's data protection responsibilities and any risks in relation to the processing of data. If you have any questions or concerns in relation to this policy or data protection in general, you should raise such matters to the attention of this person by sending an email to jpumphrey@teessidehigh.co.uk

10 How to deal with data breaches

- 10.1 The School has robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur then you must take notes and keep evidence of the breach. If the breach is likely to result in a risk to the rights and freedoms of a 'data subject' then the School must also notify the Information Commissioner's Office within 72 hours.
- 10.2 If any member of staff is made aware of a data breach, then you must contact the Finance Manager immediately by sending an email to jpumphrey@teessidehigh.co.uk and keep any evidence in relation to the breach.

11 Subject access requests

- 11.1 Data subjects can make a '**subject access request**' ('SAR') to find out what information the School holds about them. This request must be made in writing and such a request must be forwarded immediately to The Finance Manager by email to jpumphrey@teessidehigh.co.uk who will then respond accordingly.
- 11.2 The School will respond within one month to a SAR unless the request is complex in which case, the period to respond can be extended by a further two months.
- 11.3 There is no fee for making a SAR. However, if a request is manifestly unfounded or excessive the School may charge a reasonable administrative fee or refuse to respond to a request.

12 Rights of a 'Data Subject'

As a data subject;

- 12.1 You have the right to know what personal data the School processes, how it is processed and on what basis as set out in this policy.
- 12.2 You have the right to access your own personal data by way of a subject access request (SAR) (see above).
- 12.3 You have the right to correct any inaccuracies in your personal data.
- 12.4 You have the right to request that we erase your personal data where we were not entitled under the law to process it at that time, or the personal data is no longer necessary for the purpose it was collected.
- 12.5 You have the right to object to data processing where the School is relying on a legitimate interest to do so and you think that your own rights and interests outweigh the School's own and you wish for the School to stop its processing.
- 12.6 You have the right to object if we process your personal data for the purposes of direct marketing.
- 12.7 While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of processing, you can apply for its use to be restricted while the application is made.

- 12.8 You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.
- 12.9 With some exceptions, you have the right not to be subjected to automated decision-making.
- 12.10 You have the right to be notified of a data security breach concerning your personal data.
- 12.11 In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later.
- 12.12 If you have any specific questions in relation to the above rights, or you are wanting to enforce any of the rights as outlined above, you should contact the Finance Manager by sending an email to jpumphrey@teessidehigh.co.uk
- 12.13 You also have the right to complain to the Information Commissioner if you are unhappy with the School's processing of personal information. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.