Wirral Academy Trust

Data Protection Policy (GDPR)

Adopted by Board: 26 June 2018
Review Period: 2yr
Review Date: June 2020
Person responsible for policy: Data Protection Officer

INTRODUCTION

The Organisation is committed to all aspects of data protection and takes seriously its duties, and the duties of its employees. This policy sets out how the organisation deals with personal data, including personnel files and data subject access requests, and employees' obligations in relation to personal data.

As an Organisation that collects, uses and stores Personal Data about its employees, suppliers sole traders, partnerships or individuals within companies, students, governors, parents and visitors, the Organisation recognises that having controls around the collection, use, retention and destruction of Personal Data is important in order to comply with the obligations under Data Protection Laws and in particular its obligations under Article 5 of GDPR.

The Organisation has implemented this Data Protection Policy to ensure all Personnel are aware of what they must do to ensure the correct and lawful treatment of Personal Data. This will maintain confidence in the Organisation and will provide for a successful working and learning environment for all.

All Personnel will receive a copy of this Policy when they start and may receive periodic revisions of this Policy. This Policy does not form part of any member of an employee's contract of employment and the Organisation reserves the right to change this Policy at any time. All members of Personnel are obliged to comply with this Policy at all times.

If you have any queries concerning this Policy, please contact our Data Protection Officer, who is responsible for ensuring the Organisation's compliance with this Policy.

SCOPE

This Policy (and the other policies and documents referred to in it) sets out the basis on which the Organisation will collect and use Personal Data either where the Organisation collects it from individuals itself, or where it is provided to the Organisation by third parties. It also sets out rules on how the Organisation handles uses, transfers and stores Personal Data.

This Policy applies to all Personnel who collect and/or use Personal Data relating to individuals.

It applies to all Personal Data stored electronically, in paper form, or otherwise.

DEFINITIONS

The Organisation – Wirral Academy Trust [Birkenhead 6th Form College, Birkenhead Park School]

Personnel – Any employee or contractor who has been authorised to access any of the Organisation's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the Organisation.

Data Protection Laws – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

Data Protection Officer – The Data Protection Officer is John Paul Szkudlapski, Director of IT Services, and can be contacted at: jsz@bsfc.ac.uk or phone number; 01516525575

ICO – the Information Commissioner's Office, the UK's data protection regulator.

Personal Data – any information about an individual which identifies them or allows them to be identified in conjunction with other information that is held. Personal data is defined very broadly and covers both ordinary personal data from personal contact details and business contact details to special categories of personal data such as trade union membership, genetic data and religious beliefs. It also covers information that allows an individual to be identified indirectly for example an identification number, location data or an online identifier.

Special Categories of Personal Data - Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record.

DATA PROTECTION PRINCIPLES

The General Data Protection Regulation (Regulation (EU) 2016/679) and the Data Protection Act 2018 requires that eight data protection principles be followed in the handling of personal data.

These principles require that personal data must:

- be fairly and lawfully processed;
- be processed for limited purposes and not in any manner incompatible with those purposes;
- be adequate, relevant and not excessive;
- be accurate;
- not be kept longer than is necessary;
- be processed in accordance with individuals' rights;
- be secure; and
- not be transferred to countries without adequate protection.

The use of personal information

Applies to personal information that is "processed". This includes obtaining personal information, retaining and using it, allowing it to be accessed, disclosing it and, finally, disposing of it. The organisation will also ensure that the Personal Data it holds is accurate and kept up to date. If the data is inaccurate or has changed, processes will be put in place to make sure that it is erased or rectified.

All employees that collect and record Personal Data shall ensure that the Personal Data is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.

All employees that obtain and access Personal Data from sources inside/outside the organisation shall take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date and limited to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.

Lawful use of personal data

The organisation will always ensure that the collection and use of Personal Data is lawful and has assessed how it uses its Personal Data and that it complies with at least one of the lawful purposes. If this changes any time then the assessment will redone.

Personal data

Applies to information that constitutes "personal data" if it:

- identifies a person, whether by itself, or together with other information in the organisation's possession, or is likely to come into its possession; and
- is about a living person and affects that person's privacy (whether in his/her personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature.

Consequently, automated and computerised personal information about employees held by employers is covered by the Act. Personal information stored physically (for example, on paper) and held in any "relevant filing system" is also covered. In addition, information recorded with the intention that it will be stored in a relevant filing system or held on computer is covered.

A "relevant filing system" means a well-structured manual system that amounts to more than a bundle of documents about each employee filed in date order, i.e. a system to guide a searcher to where specific information about a named employee can be located easily.

The use of Sensitive personal data

The organisation will not retain sensitive personal data without the express consent of the employee in question.

The organisation will process sensitive personal data, including sickness and injury records and references, in accordance with the eight data protection principles. If the organisation enters into discussions about a merger or acquisition with a third party, the organisation will seek to protect employees' data in accordance with the data protection principles.

Transparent Processing – Privacy Notices

Please refer to our Privacy Policy and other Privacy Notices. These policies can be found on the organisations website

Data Security

The organisation takes information security very seriously and has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The organisation has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

Data Breach

The organisation will notify the ICO in the event of a Data Breach unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. Notification will take place within 72 hours of the organisation becoming aware of the breach. We will also notify the individuals affected by the Data Breach as soon as possible where the breach is likely to result in a high risk to their rights and freedoms, for example identity theft or fraud or where the breach may give rise to discrimination.

In view of the short timescale for reporting the data breach, it is important, as part of GDPR compliance, to plan for a data breach and consider matters such as how a data breach may occur, what impact it may have and how it may be rectified.

In the event of a data breach, the organisation will assess; the impact, how it may be rectified and documented, as well as encouraging disclosure through internal reporting processes.

Data subject access requests (SAR)

An employee has the right to access information kept about him/her by the organisation, including personnel files, sickness records, disciplinary or training records, appraisal or performance review notes, emails in which the employee is the focus of the email and documents that are about the employee.

The data protection officer is responsible for dealing with data subject access requests.

The organisation will not charge for allowing employees access to information about them. The organisation will respond to any data subject access request within one calendar month of the request.

The organisation will allow the employee access to hard copies of any personal information. However, if this involves a disproportionate effort on the part of the organisation, the employee shall be invited to view the information on-screen or inspect the original documentation at a place and time to be agreed by the organisation.

The organisation may reserve its right to withhold the employee's right to access data where any statutory exemptions apply.

Correction, updating and deletion of data

The organisation has a system in place that enables employees to check their personal information on a regular basis so that they can correct, delete or update any data. If an employee becomes aware that the organisation holds any inaccurate, irrelevant or out-of-date information about him/her, he/she must notify the HR department immediately and provide any necessary corrections and/or updates to the information.

Data that is likely to cause substantial damage or distress

If an employee believes that the processing of personal information about him/her is causing, or is likely to cause, substantial and unwarranted damage or distress to him/her or another person, he/she may notify the organisation in writing to the data protection officer to request the organisation to put a stop to the processing of that information.

Within 21 days of receiving the employee's notice, the organisation will reply to the employee stating either:

- that it has complied with or intends to comply with the request; or
- the reasons why it regards the employee's notice as unjustified to any extent and the extent, if any, to which it has already complied or intends to comply with the notice.

Monitoring

The organisation may monitor employees by various means including, but not limited to, recording employees' activities on CCTV, checking emails, listening to voicemails and monitoring telephone conversations. If this is the case, the organisation will inform the employee that monitoring is taking place, how data is being collected, how the data will be securely processed and the purpose for which the data will be used. The employee will usually be entitled to be given any data that has been collected about him/her. The organisation will not retain such data for any longer than is absolutely necessary.

In exceptional circumstances, the organisation may use monitoring covertly. This may be appropriate where there is, or could potentially be, damage caused to the organisation by the activity being monitored and where the information cannot be obtained effectively by any non-intrusive means (for example, where an employee is suspected of stealing property belonging to the organisation). Covert monitoring will take place only with the approval of the CEO/Principal, IT Director or the Data protection officer.

Employees' obligations regarding personal information

If an employee acquires any personal information in the course of his/her duties, he/she must ensure that:

- the information is accurate and up to date, insofar as it is practicable to do so;
- the use of the information is necessary for a relevant purpose and that it is not kept longer than necessary; and
- the information is secure.

In particular, an employee should ensure that he/she:

- uses password-protected and encrypted software for the transmission and receipt of emails;
- sends fax transmissions to a direct fax where possible and with a secure cover sheet; and
- locks files in a secure cabinet.

Where information is disposed of, employees should ensure that it is destroyed. This may involve the permanent removal of the information from the server, so that it does not remain in an employee's inbox or trash folder. Hard copies of information may need to be confidentially shredded. Employees should be careful to ensure that information is not disposed of in a wastepaper basket/recycle bin.

If an employee acquires any personal information in error by whatever means, he/she shall inform the data protection officer immediately and, if it is not necessary for him/her to retain that information, arrange for it to be handled by the appropriate individual within the organisation.

Where an employee is required to disclose personal data to any other country, he/she must ensure first that there are adequate safeguards for the protection of data in the host country. For further guidance on the transfer of personal data outside the UK, please contact the data protection officer.

An employee must not take any personal information away from the organisation's premises only in circumstances where he/she has obtained the prior consent of the data protection officer or senior management to do so.

If an employee is in any doubt about what he/she may or may not do with personal information, he/she should seek advice from their line manager or the data protection officer. If he/she cannot get in touch with their line manager or the data protection officer, he/she should not disclose the information concerned.

Consequences of non-compliance

All employees are under an obligation to ensure that they have regard to the eight data protection principles when accessing, using or disposing of personal information. Failure to observe the data protection principles within this policy may result in an employee incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal. For example, if an employee accesses another employee's employment records without the requisite authority, the organisation will treat this as gross misconduct and instigate its disciplinary procedures. Such gross misconduct will also constitute a criminal offence.

Taking employment records off site

An employee must not take employment records off site (whether in electronic or paper format) without prior authorisation from the data protection officer or senior management.

An employee may take only certain employment records off site. These are documents relating to [disciplinary or grievance meetings that cannot be held on site/meetings with occupational health or specific monitoring purposes/seeking professional advice]. An employee may also take employment records off site for any other valid reason given by the data protection officer/senior management.

Any employee taking records off site must ensure that he/she does not leave his/her laptop, other device or any hard copies of employment records on the train, in the car or any other public place. He/she must also take care when observing the information in hard copy or on-screen that such information is not viewed by anyone who is not legitimately privy to that information.

Review of procedures and training

The organisation will provide training to all employees on data protection matters on induction and on a regular basis thereafter. If an employee considers that he/she would benefit from refresher training, he/she should contact their line manager/data protection officer.

The organisation will review and ensure compliance with this policy at regular intervals.