Education Partnership Trust

Creating outstanding schools which transform learning, lives and communities

DATA PROTECTION, GDPR STATEMENT & GUIDANCE DOCUMENT.

Contents

Data Protection, GDPR - Statement & Guidance Document.

This following information sets out our commitment to achieving high standards in data protection compliance and is supported through the delivery of standards, guidance and procedures, which are documented within this statement and guidance document, alongside the Data Protection Policy, the DfE data protection toolkits for schools, the IRMS toolkit for schools and the ICO independent authority regulations which has been set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Subject Access Procedure

Right of Access

Individuals have the right to access their personal data (commonly known as subject access) and supplementary information about the processing of their data. The right of access allows individuals to be aware of and verify the lawfulness of the processing of their personal data. The information that can be requested includes:

- confirmation that their personal data is being processed
- access to a copy of the data
- the purposes of the data processing
- the categories of personal data concerned
- who the data has been, or will be, shared with
- how long the data will be stored for
- the source of the data, if not the individual
- whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

'Subject access' requests can be submitted to Lorraine Nicholls, HR Operations Manager on 01254 790026 or lnicholls@ept-uk.com in writing and must contain the name of the data subject, a correspondence address and a description of the information requested. The information will be sent without delay and at the latest within one month of receipt of the request. The school will not apply a fee to requests unless the request is manifestly unfounded or excessive. The school will take reasonable steps to verify the identification of the applicant and if the applicant wishes to request a review of the school's decision, the process for doing so will be clearly outlined in the response issued.

Third Party Access Procedure

The schools will provide information to third parties where there is a legitimate interest which means processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Manual data will be stored where it is not accessible to non-authorised third parties who do not have a legitimate reason to view or process that data. Staff should carefully consider whether they need to

take any manual data offsite before doing so and record instances where any 'special categories of data' is taken offsite along with obtaining SLT permission to do so.

The following measures must be taken by staff in relation to electronic data:

- where personal data is shared with a third party, staff should carry out due diligence and ensure the data is sent in a secure manner or appropriate measures are taken to mitigate the risk of individuals being identified
- when sending personal data to a third party, staff must carefully check the recipient and their contact details
- The school will issue regular reminders to staff and parents to ensure that personal data held is up to date and accurate. Any inaccuracies discovered should be rectified and if the inaccurate information has been disclosed to a third party; the recipients will be informed of the corrected data.
- Personal data will only be disclosed to third party organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given e.g. examination boards.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

Records Management Guidance

Records management is vital to the delivery of our services in an orderly, efficient, and accountable manner. Effective records management will help ensure that we have the right information at the right time to make the right decisions. It will provide evidence of what we do and why, therefore protecting the interests of the Schools. Records, and the information they preserve, are an important Trust asset.

We aim to balance our commitment to openness and transparency with our responsibility to deliver an effective education. Our schools will create and manage records efficiently, make them accessible where legally required, protect and store them securely and dispose of them safely at the right time.

This guidance applies to all staff, contractors, consultants and third parties who are given access to our documents and records and information processing facilities.

Review Date May 2022

We have a responsibility to ensure that our records are managed well. Different staff have different roles in relation to records management and these responsibilities are detailed below:

- Senior Information Risk Owner (SIRO) – The Chief Executive Officer has overall responsibility for managing records management risks.
- Information Asset Owners (IAOs) – this will be the Head Teacher who is responsible for ensuring that their schools have local procedures and guidance in place which comply with the records management policy and standards. IAOs will nominate a Local Records Officer (School Business Manager) to take the lead on records management issues in their areas of control.
- The SIRO is supported by specialists (BwD Information Governance team) with day to day responsibility for records management.
- All staff, contractors, consultants and third parties - everyone who receives, creates, maintains or has access to our documents and records is responsible for ensuring that they act in accordance with our records management policy, standards guidance and procedures.

Retention & Disposal Schedule

Principle F states data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Data will only be retained for the specified period outlined in the records management schedule that the school has adopted and will be destroyed in a secure manner thereafter. A copy of the records management schedule is available on https://irms.org.uk/general/custom.asp?page=SchoolsToolkit

- Toolkit for Schools – issue date 2019

Freedom of information Process

The Freedom of Information Act 2000 provides public access to information held by public authorities.

It does this in two ways:

- public authorities are obliged to publish certain information about their activities; and
- members of the public are entitled to request information from public authorities.

The Act covers any recorded information that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland. Information held by Scottish public authorities is covered by Scotland's own Freedom of Information (Scotland) Act 2002.

Public authorities include government departments, local authorities, the NHS, state schools and police forces.

Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings.

The Act does not give people access to their own personal data (information about themselves) such as their health records or credit reference file. If a member of the public wants to see information that a public authority holds about them, they should make a subject access request under the Data Protection Act 1998.

The Trust fully supports the underlying principle of the Freedom of Information Act 2000 - to provide a right of access to information held by public authorities - and is fully committed to meeting its obligations under the legislation.

Under the provisions of the Act individuals have the right to be told whether particular information exists and the right to receive the information. Upon receipt of a request for information a public authority has 20 working days in which to respond. A charge, set in accordance with the Fees Regulations defined by the Secretary of State, may be made for providing the information.

Publication Scheme

The School publication scheme commits as an authority to make information available to the public as part of its normal business activities. The information covered is included in the classes of information mentioned below, where this information is held by the School.

The Schools Publication Scheme and documents contained within the scheme are also available upon request from the School.

The Freedom of Information Act provides legal remedies against public authorities that do not comply with the legislation which can lead to fines and could ultimately be treated as contempt of court.

Personal data which falls within the scope of the Data Protection Act 1998 is not covered by the Freedom of Information 2000 and therefore not publicly accessible.

In some instances, certain personal information may be released where it relates to senior staff or staff in public facing roles, but only where such information relates to a person's working life. For example, contact information and salary grade.

The Schools Data Protection and Freedom of Information Officer (currently being undertaken by BwD Information Governance team) has responsibilities with respect to Freedom of Information as detailed below.

- To advise Schools of their responsibilities with respect to freedom of information;
- To provide guidance to the Schools in the requirements of the legislation;
- To advise the School in all matters pertaining to freedom of information;
- To ensure that arrangements are supported for dealing with requests for access;
- To establish, maintain and advise on procedures for the processing of complaints relating to freedom of information;
- To ensure that difficulties in matters related to freedom of information are promptly resolved;

Head Teachers will assist the DP & FOI Officer in the carrying out of his or her duties, the Trust requires that Head Teachers assume responsibility for those activities within their schools falling within the scope of the Act.

In particular Head Teachers must ensure that:

- the school has up to date information about departmental arrangements for dealing with Freedom of Information matters, including the contact details (Lorraine Nicholls – HR Operations Manager);
- departmental information published online is reviewed and updated as necessary;
- all information held within the school is properly documented and retrievable

- where a request for access to information has been made, the relevant data is gathered, under the direction of the DP & FOI Officer, to satisfy the request;
- staff (including casual staff) are made aware of their responsibilities and obligations with respect to information held within the department;
- information held by staff for the purpose of work or study is surrendered or, if appropriate, destroyed when the staff member or student leaves the School

Information Asset Owners (School Business Mangers and relevant Heads of Department) will assist Head Teachers in undertaking the above responsibilities. In particular, they will have responsibility for the following:

- Organising the retrieval of information from within a department in response to an access request and, in conjunction with the DP & FOI Officer, addressing any issues that may arise with respect to the application of exemptions and the need for editing of responses.

Every member of staff must comply with the Trust Freedom of Information guidelines issued by the Trust in relation to Freedom of Information.

Members of staff must refer to School Business Manager in the first instance if they receive any written request for access to information that makes specific reference to the data protection or freedom of information legislation or is for access to information that is not normally made available to an individual or to the public. Members of staff are specifically forbidden to respond to such

Schools may sometimes hire temporary staff or have dealings with external consultants (for example, computer engineers, external examiners etc.). Heads of Department must ensure that such individuals are made aware of their responsibilities and obligations under the Freedom of Information Act 2000 and are

FOI: charges for information requests

Some information is available free, but for some there may be a charge. Charges vary according to type of information requested.

Freedom of Information charges

If you are making a request for information that is not readily available, then you may be charged a fee.

FOI requests which will cost less than £450 to answer will be free of charge (please note: we may charge for the cost of postage, photocopying and so on). The £450 cost is based on a calculation of time at £25 per hour of officer time. If you refuse to pay the fee, the School can refuse to supply the information.

Information Security Policy

Principle F states data should be processed in a manner that ensures appropriate security of the personal data. This means the school must have appropriate security to prevent the personal data it holds being accidentally or deliberately compromised. Particular attention will be paid to the need for security of sensitive personal data.

Manual data will be stored where it is not accessible to anyone who does not have a legitimate reason to view or process that data. Staff should carefully consider whether they need to take any manual

data offsite before doing so and record instances where any 'special categories of data' is taken offsite. The following measures must be taken by staff in relation to electronic data:

- portable electronic devices, such as laptops, iPad's and hard drives that contain personal data are stored in a locked cupboard or drawer
- encryption software is used to protect all portable devices and removable media that contain personal data, such as laptops and USB devices
- passwords must meet appropriate security standards, be changed at regular intervals and must not be divulged to any other persons
- where personal data is shared with a third party, staff should carry out due diligence and ensure the data is sent in a secure manner or appropriate measures are taken to mitigate the risk of individuals being identified
- when sending personal data to a third party, staff must carefully check the recipient and their contact details
- where personal devices are used to access organisational email accounts, staff should ensure appropriate passwords are applied to the device and they access the accounts by the recommended means i.e. Office 365 users should use the Office 365 application rather than syncing to phone
- staff should not open links when emails are received from unknown recipients or the emails appear suspicious
- personal data must be stored in a secure and safe manner, with careful consideration made to who can access the data

IT Acceptable Use Policy

The School Network may not be used directly or indirectly by a User for the download, creation, manipulation, transmission or storage of:

- any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;
- unsolicited "nuisance" emails;
- material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of the University or a third party;
- material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation;
- material with the intent to defraud or which is likely to deceive a third party;
- material which advocates or promotes any unlawful act;
- material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or
- material that brings the University into disrepute.

The School Network must not be deliberately used by a User for activities having, or likely to have, any of the following characteristics:

- intentionally wasting staff effort or other School resources;
- corrupting, altering or destroying another User's data without their consent;

- disrupting the work of other Users or the correct functioning of the School Network; or
- pursuance of commercial activities (even if in support of school business), subject to a range of exceptions.

Users shall not:

- introduce data-interception, password-detecting or similar software or devices to the Schools Network;
- seek to gain unauthorised access to restricted areas of the School Network;
- access or try to access data where the user knows or ought to know that they should have no access;
- carry out any hacking activities; or
- intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.

Consequences of Breach

In the event of a breach of this Acceptable Use Policy by a User the School may in its sole discretion:

- restrict or terminate a User's right to use the School Network;
- withdraw or remove any material uploaded by that User in contravention of this Policy; or
- where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.

In addition, where the User is also a member of the school staff, the school may take such action, disciplinary or otherwise as it deems appropriate and which is in accordance with its Disciplinary procedures.

CCTV Policy

Not all schools within the Trust use CCTV, however the Trust makes provision for every eventually and each school will complete their own CCTV policy.