DIXONS ACADEMIES TRUST

GDPR Data Protection Policy

Responsibility for Review: Executive Principal, Dixons Academies Trust
Date of Last Review: September 2018

Contents

Statement of intent

Dixons Academies Charitable Trust (DMAT) is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the EU's General Data Protection Regulation (GDPR).

DMAT may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the Local Authority, other academies and educational bodies, and potentially children's services.

This policy is in place to ensure that all staff and governors are aware of their responsibilities and outlines how DMAT complies with the following core principles of the GDPR. All employees and volunteers of the DMAT must be made aware of the Trust policy and procedures and must provide written acknowledge of their understanding of their individual responsibilities in relation to the GDPR.

All data held by DMAT and its academies are the responsibility of the Trust.

Organisational methods for keeping data secure are imperative, and DMAT believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the GDPR, which will come into effect on 25 May 2018. The government have confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

1.0 Legal framework

1.1. This policy has due regard to legislation, including but not limited to the following:

- the General Data Protection Regulation
- the Freedom of Information Act 2000
- the Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- DMAT Standards and Framework Act 1998

1.2. This policy also has regard to the following guidance:

- ICO (2018) 'Guide to the General Data Protection Regulation (GDPR)'

1.3. This policy will be implemented in conjunction with the following other Trust policies:

- Photography and Videos at Academy Policy
- E-Security Policy
- Freedom of Information Policy
- CCTV Policy

2.0 Applicable data

2.1 For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g., an Internet Protocol (IP) address. The GDPR applies to both automated personal data and to manual filing systems, where personal data are accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g., key-coded.

2.2 Sensitive personal data are referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data, and data concerning health matters.

3.0 Principles

3.1 In accordance with the requirements outlined in the GDPR, personal data will be:

- processed lawfully, fairly, and in a transparent manner in relation to individuals
- collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes
- adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, when necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures

3.2 The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

4.0 Accountability

4.1 DMAT will implement appropriate technical and organisational measures to demonstrate that data are processed in line with the principles set out in the GDPR.

4.2 DMAT will provide comprehensive, clear, and transparent privacy policies.

4.3 Additional internal records of DMAT's processing activities will be maintained and kept up to date.

4.4 Records of activities relating to higher-risk processing will be maintained, such as the processing of activities that:

- are not occasional
- could result in a risk to the rights and freedoms of individuals
- involve the processing of special categories of data or criminal conviction and offence data

4.5 Internal records of processing activities will include the following:

- name and details or the organisation
- purpose(s) of the processing
- description of the categories of individuals and personal data
- retention schedules
- categories of recipients of personal data
- description of technical and organisational security measures
- details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

4.6 DMAT will implement measures that meet the principles of data protection by design and data protection by default, such as:

- data minimisation
- pseudonymisation
- transparency
- allowing individuals to monitor processing
- continuously creating and improving security features

4.7 Data protection impact assessments will be used, when appropriate.

5.0 Data protection officer (DPO)

5.1 A DPO will be appointed in order to:

- inform and advise DMAT and its employees about their obligations to comply with the GDPR and other data protection laws
- monitor DMAT'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

5.2 An existing employee will be appointed to the role of DPO provided that this person's duties are compatible with the duties of the DPO and do not lead to a conflict of interests. For DMAT, this role will report to the Trust COO.

5.3 The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to academies.

5.4 The DPO will report to the highest level of operational management at the Trust, which is the Trust COO.

5.5 The DPO will operate independently and will not be dismissed or penalised for performing his or her task.

5.6 Sufficient resources will be provided to the DPO to enable that person to meet the requisite GDPR obligations.

6.0 Lawful processing

6.1 The legal basis for processing data will be identified and documented prior to data being processed.

6.2 Under the GDPR, data will be lawfully processed under the following conditions:

- the consent of the data subject has been obtained
- processing is necessary for:
  - compliance with a legal obligation
  - the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
  - the performance of a contract with the data subject or to take steps to enter into a contract
  - protecting the vital interests of a data subject or another person
  - the purposes of legitimate interests pursued by the controller or a third party, except when such interests are overridden by the interests, rights, or freedoms of the data subject. (This condition is not available to processing undertaken by DMAT in the performance of its tasks)

6.3 Sensitive data will be processed only under the following conditions:

- explicit consent of the data subject has been obtained, unless reliance on consent is prohibited by EU or Member State Law
- processing is carried out by a not-for-profit body with a political, philosophical, religious, or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- processing relates to personal data:
  - carrying out obligations under employment, social security or social protection law, or a collective agreement
  - protecting the vital interests of a data subject or another individual when the data subject is physically or legally incapable of giving

consent

– the establishment, exercise, or defence of legal claims or when courts are acting in their judicial capacity

– reasons of substantial public interest on the basis of Union or Member State law, which is proportionate to the aim pursued and which contains appropriate safeguards

– the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

– reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medicinal products or medical devices

– archiving purposes in the public interest, or scientific and historical research purposes, or statistical purposes in accordance with article 89(1)

7.0 Consent

7.1 Consent must be a positive indication. It cannot be inferred from silence, inactivity, or pre-ticked boxes.

7.2 Consent will be accepted only when it is freely given, specific, informed, and an unambiguous indication of the individual's wishes.

7.3 When consent is given, a record will be kept documenting how and when consent was given.

7.4 DMAT ensures that consent mechanisms meet the standards of the GDPR. When the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

7.5 Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be re-obtained.

7.6 Consent can be withdrawn by the individual at any time.

7.7 When a child is under the age of 16 [or younger if the law provides it (up to the age of 13)], the consent of parents will be sought prior to the processing of their data, except when the processing is related to preventative or counselling services offered directly to a child.

8.0 The right to be informed

8.1 The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language that is concise, transparent, easily accessible, and free of charge.

8.2 If services are offered directly to a child, DMAT will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

8.3 In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- the identity and contact details of the controller (and when applicable, the controller's representative) and the DPO
- the purpose of, and the legal basis for, processing the data
- the legitimate interests of the controller or third party
- any recipient or categories of recipients of the personal data
- details of transfers to third countries and the safeguards in place
- the retention period of criteria used to determine the retention period
- the existence of the data subject's rights, including the right to:
  - withdraw consent at any time
  - lodge a complaint with a supervisory authority
- the existence of automated decision making, including profiling, how decisions are made, the significance of the process, and the consequences

8.4 When data are obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

8.5 When data are not obtained directly from the data subject, information regarding the categories of personal data that DMAT holds, the source that the personal data originates from, and whether it came from publicly accessible sources, will be provided.

8.6 For data obtained directly from the data subject, this information will be supplied at the time the data are obtained.

8.7 In relation to data that are not obtained directly from the data subject, this information will be supplied:

- within one month of having obtained the data
- if disclosure to another recipient is envisaged, at the latest, before the data are disclosed
- if the data are used to communicate with the individual, at the latest, when the first communication takes place

9.0 The right of access

9.1 Individuals have the right to obtain confirmation that their data are being processed.

9.2 Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

9.3 DMAT will refer ALL requests for information to the Trust DPO.

9.4 The Trust may impose a 'reasonable fee' to comply with requests for information.

9.5. When a SAR has been made electronically, the information will be provided in a commonly used electronic format.

9.6 When a request is manifestly unfounded, excessive, or repetitive, a reasonable fee will be charged.

9.7 All fees will be based on the administrative cost of providing the information.

9.8 All requests will be responded to without delay, and at the latest, within one month of receipt.

9.9 In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

9.10 When a request is manifestly unfounded or excessive, DMAT holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as that person's right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

9.11 In the event that a large quantity of information is being processed about an individual, DMAT will ask the individual to specify the information the request is in relation to.

10.0 The right to rectification

10.1 Individuals are entitled to have any inaccurate or incomplete personal data rectified.

10.2 When the personal data in question have been disclosed to third parties, DMAT will inform the individual of the rectification where possible.

10.3 When appropriate, DMAT will inform the individual about the third parties that the data have been disclosed to.

10.4 Requests for rectification will be responded to within one month; this will be extended by two months when the request for rectification is complex.

10.5 When no action is being taken in response to a request for rectification, DMAT will explain the reason for this to the individual and will inform the individual of his or her right to complain to the supervisory authority and to a judicial remedy.

11.0 The right to erasure

11.1 Individuals hold the right to request the deletion or removal of personal data when there is no compelling reason for its continued processing.

11.2 Individuals have the right to erasure in the following circumstances:

- when the personal data are no longer necessary in relation to the purpose for which they were originally collected/processed
- when the individual withdraws his or her consent
- when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- when the personal data were unlawfully processed
- when the personal data are required to be erased in order to comply with a legal obligation
- when the personal data are processed in relation to the offer of information society services to a child

11.3 DMAT has the right to refuse a request for erasure when personal data are being processed for the following reasons:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority
- for public health purposes in the public interest
- for archiving purposes in the public interest, scientific research, historical research, or statistical purposes
- the exercise or defence of legal claims

11.4 As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations in which a child has given consent to processing and the individual later requests erasure of the data, regardless of age at the time of the request.

11.5 When personal data have been disclosed to third parties, the individual will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

11.6 When personal data have been made public within an online environment, DMAT will inform other organisations that process the personal data to erase links to and copies of the personal data in question.

12.0 The right to restrict processing

12.1 Individuals have the right to block or suppress DMAT's processing of personal data.

12.2 In the event that processing is restricted, DMAT will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

12.3 DMAT will restrict the processing of personal data in the following circumstances:

- when an individual contests the accuracy of the personal data, processing will be restricted until DMAT has verified the accuracy of the data
- when an individual has objected to the processing and DMAT is considering whether its legitimate grounds override those of the individual
- when processing is unlawful and the individual opposes erasure and requests restriction instead
- when DMAT no longer needs the personal data but the individual requires the data to establish, exercise, or defend a legal claim

12.4 If the personal data in question have been disclosed to third parties, DMAT will inform the individual about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

12.5 DMAT will inform individuals when a restriction on processing has been lifted.

13.0 The right to data portability

13.1 Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

13.2 Personal data can be easily moved, copied, or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

13.3 The right to data portability applies only in the following cases:

- to personal data that an individual has provided to a controller
- when the processing is based on the individual's consent or for the performance of a contract
- when processing is carried out by automated means

13.4 Personal data will be provided in a structured, commonly used, and machine-readable form.

13.5 DMAT will provide the information free of charge.

13.6 When feasible, data will be transmitted directly to another organisation at the request of the individual.

13.7 DMAT is not required to adopt or maintain processing systems that are technically compatible with other organisations.

13.8 In the event that the personal data concern more than one individual, DMAT will consider whether providing the information would prejudice the rights of any other individual.

13.9 DMAT will respond to any requests for portability within one month.

13.10 When the request is complex, or a number of requests have been received, the time frame can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

13.11 When no action is being taken in response to a request, DMAT will, without delay and at the latest within one month, explain to the individual the reason for this and will inform the individual of his or her right to complain to the supervisory authority and to a judicial remedy.

14.0 The right to object

14.1 DMAT will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

14.2 Individuals have the right to object to the following types of data processing:

- processing based on legitimate interests or the performance of a task in the public interest
- direct marketing
- processing for purposes of scientific or historical research and statistics

14.3 When personal data are processed for the performance of a legal task or legitimate interests,

- An individual's grounds for objecting must relate to his or her particular situation
- DMAT will stop processing the individual's personal data unless the processing is for the establishment, exercise, or defence of legal claims, or when DMAT can demonstrate compelling legitimate grounds for the processing, which override the interests, rights, and freedoms of the individual

14.4 When personal data are processed for direct marketing purposes,

- DMAT will stop processing personal data for direct marketing purposes as soon as an objection is received
- DMAT cannot refuse an individual's objection regarding data that are being processed for direct marketing purposes

14.5 When personal data are processed for direct marketing purposes,

- the individual must have grounds relating to that person's particular situation in order to exercise his or her right to object
- when the processing of personal data is necessary for the performance of a public interest task, DMAT is not required to comply with an objection to the processing of the data

14.6 When the processing activity is outlined above but is carried out online, DMAT will offer a method for individuals to object online.

15.0 Automated decision making and profiling

15.1 Individuals have the right not to be subject to a decision when

- it is based on automated processing, e.g., profiling
- it produces a legal effect or similarly significant effect on the individual

15.2 DMAT will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

15.3 When automatically processing personal data for profiling purposes, DMAT will ensure that the appropriate safeguards are in place, including:

- ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact
- using mathematical or statistical procedures
- implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and to minimise the risk of errors
- securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects

15.4 Automated decisions must not concern a child or be based on the processing of sensitive data, unless

- DMAT has the explicit consent of the individual
- the processing is necessary for reasons of substantial public interest on the basis of Union/Member State Law

16.0 Privacy by design and privacy impact assessments

16.1 DMAT will act in accordance with the GDPR by adopting a privacy-by-design approach and implementing technical and organisational measures that demonstrate how DMAT has considered and integrated data protection into processing activities.

16.2 Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with DMAT's data protection obligations and meeting individuals' expectations of privacy.

16.3 DPIAs will allow DMAT to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to DMAT's reputation, which might otherwise occur.

16.4 A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

16.5 A DPIA will be used for more than one project, when necessary.

16.6 High-risk processing includes but is not limited to the following:

- systematic and extensive processing activities, such as profiling
- large-scale processing of special categories of data or personal data, which is in relation to criminal convictions or offences

16.7 DMAT will ensure that all DPIAs include the following information:

- a description of the processing operations and the purposes
- an assessment of the necessity and proportionality of the processing in relation to the purpose
- an outline of the risks to individuals
- the measures implemented in order to address risk

16.8 When a DPIA indicates high-risk data processing, DMAT will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

17.0 Data breaches

17.1 The term 'personal data breach' refers to a breach of security that has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

17.2 The Principal will ensure that all staff members are made aware of and understand what constitutes a data breach as part of their CPD training.

17.3 When a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

17.4 All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of DMAT becoming aware of them.

17.5 The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

17.6 In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, DMAT will notify those concerned directly.

17.7. A 'high-risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

17.8 In the event that a breach is sufficiently serious, the public will be notified without undue delay.

17.9 Effective and robust breach detection, investigation, and internal reporting procedures are in place at DMAT, which facilitate decision making in relation to whether the relevant supervisory authority or the public need to be notified.

17.10 Within a breach notification, the following information will be outlined:

- the nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- the name and contact details of the DPO
- an explanation of the likely consequences of the personal data breach
- a description of the proposed measures to be taken to deal with the personal data breach
- when appropriate, a description of the measures taken to mitigate any possible adverse effects

17.11 Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

17.12 DMAT Breach Procedures are detailed in Appendix 1.

18.0 Data security

18.1 Confidential paper records will be kept in a locked filing cabinet, drawer, or safe, with restricted access.

18.2 Confidential paper records will not be left unattended or in clear view anywhere with general access.

18.3 Digital data are coded, encrypted, or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

18.4 When data are saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer, or safe when not in use.

18.5 Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted. DMAT does not permit the use of memory sticks for any of the data that it is accountable for.

18.6 All electronic devices are password-protected to protect the information on the device in case of theft.

18.7 When possible, DMAT enables electronic devices to allow the remote blocking or deletion of data in case of theft.

18.8 Staff and governors will not use their personal emails for academy purposes. All staff and governors will have a Trust email address that should be used for all academy/Trust work.

18.9 All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

18.10 Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

18.11 Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

18.12 When sending confidential information by fax, staff will always check that the recipient is correct before sending.

18.13 When personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g., keeping devices under lock and key. The person taking the information from DMAT premises accepts full responsibility for the security of the data.

18.14 Before sharing data, all staff members will ensure that:

- they are allowed to share them
- adequate security is in place to protect them
- who will receive the data has been outlined in a privacy notice

18.15 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of DMAT containing sensitive information are supervised at all times.

18.16 The physical security of DMAT's buildings and storage systems, and access to them, is reviewed on a timely basis. If an increased risk of vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

18.17 DMAT takes its duties under the GDPR seriously, and any unauthorised disclosure may result in disciplinary action.

18.18 The DPO is responsible that continuity and recovery measures are in place to ensure the security of protected data.

19.0 Publication of information

19.1 DMAT publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- policies and procedures
- minutes of meetings
- annual reports
- financial information

19.2 Classes of information specified in the publication scheme are made available quickly and easily on request.

19.3 DMAT will not publish any personal information, including photos, on its website without the permission of the affected individual.

19.4 When uploading information to a DMAT website, staff are considerate of any metadata or deletions that could be accessed in documents and images on the site.

20.0 CCTV and photography

20.1 DMAT understands that recording images of identifiable individuals constitutes the processing of personal information, so it is done in line with data protection principles.

20.2 DMAT notifies all pupils, staff, and visitors of the purpose for collecting CCTV images via notice boards, letters, and email.

20.3 Cameras are placed only where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

20.4 All CCTV footage will be kept for six months for security purposes; the OPS Manager is responsible for keeping the records secure and allowing access.

20.5 DMAT will always indicate its intentions for taking photographs of pupils and will secure permission before publishing them.

20.6 If DMAT wishes to use images/video footage of pupils in a publication, such as a DMAT website, prospectus, or recordings of Academy plays, written permission will be sought for the particular usage from the parent of the pupil.

20.7 Precautions are taken, as outlined in the Photography and Videos at Academy Policy, when publishing photographs of pupils in print, video, or on a DMAT website.

20.8 Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

21.0 Data retention

21.1 Data will not be kept for longer than is necessary.

21.2 Unrequired data will be deleted as soon as practicable.

21.3 Some educational records relating to former pupils or employees of DMAT may be kept for an extended period for legal reasons but also to enable the provision of references or academic transcripts.

21.4 Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

22.0 DBS data

22.1 All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

22.2 Data provided by the DBS will never be duplicated.

22.3 Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

23.0 Policy review

23.1 This policy is reviewed every two years by the COO.

The next scheduled review date for this policy is September 2019.

Apendix 1

Take care when dealing with student and staff data

Personal data is an individual's name and any other piece of identifying information – see below for examples of personal data handled in schools.

- Address details
- SEN status
- Free School Meals eligibility
- Pupil Premium
- Educational levels and results (Inc. mock / practice exam papers / pieces of work with comments / feedback)
- Child protection details
- Witness / incident details
- Accident records
- Photographs
- Staff payroll / salary information
- Staff performance management details

Top tips to keep data safe

- Documents containing personal data should be shredded or placed in the confidential waste consoles.
- Do not leave documents printing which contain personal data. If the printer jams, report this immediately and do not leave until the jam has been cleared.
- If something personal is left on the printer, or somewhere public, pass it on to the Operations & Business Manager who will report it to the DPO.
- Take care when using electronic whiteboards in classrooms – registers often show FSM, SEN alerts etc.
- Take care not to inadvertently display other students' results / grades if using lists at Parent Evenings.
- Ensure you confirm the identity of callers and email addresses before discussing personal data.
- Where it is necessary to send data elsewhere, send it securely e.g. encrypted document / email / Secure Access S2S or BSO Dropbox.
- Keep your working area and desk tidy and do not leave documents out for others to see. Always lock away confidential information in a lockable cupboard / filing cabinet.
- Take care not to display personal data if visitors and students regularly use your office.
- Lock your PC / laptop when not in use – especially in classrooms and public areas.
- Do not share your passwords with anyone; keep them safe in a password protected document on your PC / laptop.
- Do not use portable external devices i.e. memory sticks / external hard drives. All documents are to be saved to the desk top / one drive.
- New software requests must be submitted to the IT helpdesk to ensure they are compliant and compatible. The form is available on the SharePoint site under GDPR.
- If you access work emails on your mobile phone, you are responsible to ensure that data cannot be seen or accessed by anyone else. Please remember that most coffee shops i.e. Costa have unsecure Wi-Fi networks.
- When you are sending an email to a number of people outside of the organisation i.e. suppliers, please ensure you put them in BCC (Blind Carbon Copy) so their email addresses are not visible to each other.
- Check the school holds signed Privacy Notices before sharing any data covered by the Privacy Notices.

Trust Data Breach Management Procedure

DATA BREACHES SHOULD BE REPORTED IMMEDIATELY TO

THE SCHOOL (ACADEMY OPERATIONS & BUSINESS MANAGER, HEAD OF IT/PRINCIPAL) AND THE DATA PROTECTION OFFICER (DPO) - TEL: 01274 424350 / EXT 2453 E: GDPR@dixonsat.com

GIVE AS MUCH INFORMATION AS POSSIBLE

THE DATA BREACH WILL BE LOGGED ON THE TRUST BREACH REGISTER BY THE DATA PROTECTION OFFICER

IF DETERMINED TO BE ICO NOTIFIABLE, THE ICO WILL BE NOTIFIED WITHIN 72 HOURS BY THE DATA PROTECTION OFFICER

IN ALL CASES, AN INVESTIGATION WILL BE IMPLEMENTED BY THE DATA PROTECTION OFFICER

RECOMMENDATIONS FOR IMPROVEMENT WILL BE SHARED AND CONTROL MEASURES IMPLEMENTED

Examples of data breaches within the school environment