TBAP
Multi-Academy Trust

General Data Protection Regulation Guidelines

2019 - 20

Policy dates: ***September 2019 – August 2020***
Staff Lead: ***Jo Sennitt***
Trustee Lead:
Policy approved: ***Board meeting June 2019***
Next review date: ***March 2020;***
(Jan 2020 new DPO added)

TBAP AP AND SPECIAL ACADEMIES

WEST
COURTYARD
LATIMER
BEACHCROFT
BRIDGE
16-19
OCTAGON
CAMBRIDGE
UNITY
OCTAVIA
ASPIRE
EAST

NORTH WEST
NEW HORIZONS
CSS Commissioning & School Support
TBAP Teaching School Alliance
tbapfoundation EVERY CHILD A CHANCE
SUPPORT

These guidelines should be read in conjunction with the TBAP Data Protection Policy and the E-learning Safe use Policy.

Strategic and operational practices

Within the Trust:

- The Heads of School are the Senior Information Risk Officer (SIRO).
- IT Manager is the Data Controller (DC) with responsibility for overseeing data protection compliance.
- Learners are issued with TBAP's pupil privacy notice (Appendix 1)
- Staff are issued with TBAP's staff privacy notice (Appendix 2)
- Staff are clear who the key contact(s) for key school information are (the Information Asset Owners).
- We ensure staff know to immediately report, and who to report to, any incidents where data protection may have been compromised, such as when passwords for sensitive systems or devices are lost or stolen, so that relevant action(s) can be taken.
- All staff are DBS checked and records are held in one central record within a spreadsheet located in the Shared Drive but permissions given to each responsible person.

  We ensure ALL the following school stakeholders sign an Acceptable Use Agreement (Appendix 3). We have a system so we know who has signed.

  - staff
  - governors
  - volunteers

  This makes clear all responsibilities and expectations with regard to data security.

  Pupils and parents should sign a copy of the E-learning Safe Use Policy.
- We have approved educational web filtering across our wired and wireless networks. We also have Impero Software as an additional layer of monitoring software across our network system. We monitor school e-mails/blogs/online platforms, etc. to ensure compliance with the Acceptable Use Agreement. As well as monitoring usage, we may also monitor content of e-mails / blogs / etc.
- We follow TBAP Trust guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private.
- We require staff to use STRONG passwords for access into our MIS system.
- We require staff to change their passwords into the MIS, Office 365, Windows Computer login every 90 days.
- We require that any personal/sensitive material must be encrypted if the material is to be removed from the school, and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff who set up usernames and passwords for e-mail, network access, Office365 work within the approved system and follow the security processes required by those systems.
- We ask staff to undertake house-keeping checks at least annually to review, remove and destroy any digital materials and documents which need no longer be stored.

- A GDPR checklist is also attached to ensure regular compliance (Appendix 4)

Technical or manual solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 20 mins. idle time.
- We use OneDrive for Business if any member of staff has to take any sensitive information off site.
- We use RAv3 / VPN solution with its 2-factor authentication for remote access into our systems.
- We use the DfE S2S site to securely transfer CTF pupil data files to DfE / other schools.
- We use the Pan-London Admissions system to transfer admissions data. <Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.>
- We use LGfL Egress to transfer documents to schools in London, such as references, reports of children.
- We use Microsoft OneDrive for Business as well as Microsoft Sharepoint for online document storage.
- We store any sensitive/special category written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- We create backups on servers using Acronis Software. No back-up tapes or External Hard Drives leave the site on mobile devices.
- We use Acronis Backup for disaster recovery on our as well as server replication on two different sites as our backup solution.
- We comply with the WEEE directive on equipment disposal, by using an approved disposal company for disposal of IT equipment. For systems, where any protected or restricted data has been held, (such as servers, photocopiers), we get a certificate of secure deletion.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using a cross-cut shredder.

APPENDIX 1

Privacy Notice (How we use pupil information)

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, and country of birth)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Relevant medical information
- Special educational needs information (where applicable)
- Exclusions
- Behavioural information
- Careers information

Why we collect and use this information

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- to register pupils with examination boards

The lawful basis on which we use this information

We collect and use pupil information under the Education Act 1996 and we ask pupils to give us consent to the processing of his or her personal data for one or more specific purposes processing is carried out in the course of its legitimate activities with appropriate safeguards by the Trust.

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

We hold pupil data for as long as the pupil is with us.

Who we share pupil information with

We routinely share pupil information with:

- schools and colleges that the pupils attend after leaving us
- work experience placement organisations
- our local authority
- the Department for Education (DfE)
- Educational Psychologist (where appropriate)
- School Nurse
- Therapists where the service is bought in
- Trustees and Governors

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with the (DfE) under regulation 4 and 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Youth support services

Pupils aged 13+

Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age 16.

Pupils aged 16+

We will also share certain information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our local authority website.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

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

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases 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 store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the Head of School or the Data Protection Officer.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact our Data Protection Officer

Details of the DPO
The DPO is an organisation

Name
Judicium Consulting Limited

Address
72 Cannon Street, London EC4N 6AE

Email dataservices@judicium.com

Tel. 020 3326 9174

APPENDIX 2

Privacy Notice (How we use school workforce information)

The categories of school workforce information that we collect, process, hold and share include:

- personal information (such as name, employee or teacher number, national insurance number)
- special categories of data including characteristics information such as gender, age, ethnic group
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- medical fit notes
- qualifications (and, where relevant, subjects taught)
- Occupational health reports
- Performance information

Why we collect and use this information

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid
- managing absence
- managing performance and payment of any performance related pay and/or bonuses

The lawful basis on which we process this information

We process this information under the Education Act 1996 for the purposes of the school workforce census and we ask staff to give us consent to the processing of his or her personal data for one or more specific purposes processing is carried out in the course of its legitimate activities with appropriate safeguards by the Trust.

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information

We hold school workforce data for 7 years unless there is a specific safeguarding reason why certain information for an individual has to be retained.

Who we share this information with

We routinely share this information with:

- our local authority
- the Department for Education (DfE)
- our external Payroll bureau
- statutory agencies where this is a legal requirement

Why we share school workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority
We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)
We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

We are required to share information about our pupils with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

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
-

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of

the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold, although as a current employee you are able to access your information on the Select HR self-service system. To make a formal request for your personal information, contact the Resources Director.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Further information

If you would like to discuss anything in this privacy notice, please contact:

- a member of the TBAP Human Resources Team

APPENDIX 3

ACCEPTABLE USE AGREEMENT

Data Security – Do's and Don'ts for school staff

Passwords – Do

- use a strong password (see the National Cyber Security Centre advice)

Passwords – Don't

- share your passwords with anyone else or write them down
- save passwords in web browsers if offered to do so

Devices – Do

- try to prevent people seeing you enter passwords or view sensitive information
- log-off / lock your device when leaving it unattended

Devices – Don't

- use personal devices to view school-related or pupil data

Sending and sharing – Do

- be aware of who you are allowed to share information with. Check with your school Data Controller if you are not sure, who will check that third parties are GDPR-compliant
- only use encrypted removable media (such as encrypted USB pen drives) if ever taking any personal or sensitive data outside your school (which should be avoided and only done with permission)

Sending and sharing – Don't

- send sensitive information (even if encrypted) on removable media (USB drives, CDs, portable drives), if secure remote access is available.
- send sensitive information by email unless it is encrypted and use the systems that you are told to use

Accessing / saving data – Do

- only attempt to access data you are allowed to and save it on locations where your school knows that data is stored (the school must know where all data is and be able to access it)

Working on-site – Don't

- leave sensitive information unattended; lock it away in lockable drawers or log off or lock your work station
- let strangers or unauthorised people into staff areas
- position screens where they can be read from outside the room.

Working off-site – Do

- only take information offsite when you are authorised to and only when it is necessary. Ensure that it is protected offsite in the ways referred to above
- access data remotely instead of taking it off-site using approved secure systems
- make sure you sign out completely from any services you have used
- ensure you save to the appropriate directory to enable regular backups

I AGREE AS A STAFF MEMBER, VOLUNTEER, LAB MEMBER, RAB MEMBER, TRUSTEE THAT I ACCEPT THE TERMS OF THIS ACCEPTABLE USE AGREEMENT AND ABIDE BY THE CONTENT

SIGNED……

DATED…….

APPENDIX 4

Data handling check list for compliance & best practice

Introduction

Schools have a duty under the 1998 Data Protection Act to ensure that personal data is stored and accessed securely. Schools also have a need to meet the General Data Protection Regulations (GDPR), which will be enforced from 25 May 2018. Personal data includes information in any form (text, images) relating to an identified or identifiable pupil or member of staff. Data protection legislation applies to paper records as well as electronically stored data.

Data protection legislation requires access to personal data to be strictly controlled and also for the integrity of the data to be maintained. This requires the data to be secured against loss through systems failure and also loss through theft of computer equipment or storage media, together with irreparable damage to hardware or media due to, for example, fire or flood.

It is recognised that this is not always easy to fully implement owing to conflict with other existing policy, practice and the limits of some technology.

Strategic		
☐ Ensure school registers every 3 years with the Information Commissioner's Office(ICO)[1] ☐ Appoint a named Senior Information Risk Officer (SIRO). This could be the Head of School. ☐ Appoint a named Data Protection Officer (DPO) with responsibility for data protection compliance. This should be a discrete appointment and must avoid conflicts of interest (see DPO FAQs document at gdpr.lgfl.net ☐ Consider whether to conduct a Data Protection Impact Assessment, especially prior to the implementation of new processing activities or new IT systems[2]. ☐ Make sure ALL staff are fully aware of, and understand the implications of, the school's Acceptable Use Agreement and Policy (AUP), and its updates and have signed anagreement. ☐ Make sure ALL staff have Disclosure and Barring (DBS) checks in-place (formally CRB) and keep your data as a Single Central Record (preferably in your MIS, such as SIMS Personnel)[3]. ☐ Ensure all data subjects (staff, learners and parents where applicable) are aware of what data is being held about them, for what purpose and how it is used by issuing privacy or fair processing notices[4]. ☐ Ensure contracts for employment state that misuse of data is a disciplinarymatter. ☐ Identify your information 'assets' (e.g. HR data, exam data, student contact data) and for each one, identify an Information Asset Owner (IAO). Check the risks and controls on those data assets. There is a data asset audit/log template at gdpr.lgfl.net to help you with this. ☐ Have strategies for managing and recovering from incidents where information at risk, *i.e. who to contact, where to get advice, how communicate, etc.* ☐ Have procedures in place to detect, investigate and report a data breach to the ICOwhen necessary[5] (within 72 hours under GDPR).		

TBAP
Multi-Academy Trust

TBAP
Multi-Academy Trust

Transferring data		

- ☐ Protectively mark documents (electronic or paper) that are sensitive
- ☐ Do not send sensitive data across unencrypted routes and if no alternative is available, take sensible precautions (e.g. password protect the file and send the password separately) or don't send it.
- ☐ Never just 'forward' sensitive documents/data out of one email system to another email system without protecting the data. Care should be taken to ensure the email is correctly addressed.
- ☐ Only transfer documents with the Local Authority / Health and Welfare services using a Local Authority approved secure transit (usually not email).
- ☐ Do not use personal computer systems or personal email addresses; these may not have adequate security protection.
- ☐ Try to avoid sending anything sensitive by fax (this old technology is still sometimes requested!), be careful to dial correctly and take steps to ensure the intended recipient has received the information as soon as possible after sending the message.
- ☐ If sending through post - double bag and mark the inside bag confidential/sensitive. Consider using courier / recorded post if particularly sensitive.

Staff practices		

- ☐ Ensure staff accessing sensitive data know to use complex (strong) passwords, change them regularly and keep such passwords unique.
- ☐ Staff should never share passwords.
- ☐ Ensure staff do not take any data off site that is not on an encrypted device and minimise the need to ever take data off-site. Treat paper copies with the same care.
- ☐ Staff should lock computer screens or log-off when away from the computer.
- ☐ Ensure staff are aware of their responsibilities - data security issues and risks, and know who to report to when information put at risk (e.g. USB key lost, folder of contact details mislaid) – and provide periodic refresher training.
- ☐ Do not permit staff to store / hold pupil or staff data on any device that is not owned by the school or part of the school network (such as personal cameras, laptops, smart phones, personal 'drop boxes', etc.)

Administration practices		

- ☐ Ensure data is updated regularly so it is as accurate as possible.
- ☐ Ensure filing cabinets used to stored sensitive documents are locked.
- ☐ Shred sensitive paper documents when no longer required, e.g. at end of meetings; preferably use a cross cutter shredder.
- ☐ Only transfer pupil data (CTFs) using the DFE secure method (S2S).
- ☐ Only transfer Key Stage and Census returns to via the approved system
- ☐ When printing or photocopying documents, don't leave copies behind and take care to ensure you collect the correct number of pages and the originals.
- ☐ Use the Pan-London Admissions System (combined with OTP tag).

Technical systems	Person Responsible:	Next review date:

- ☐ Dispose of equipment following WEEE (Waste Electrical and Electronic Directive[6]). Ensure the disposer/recycler securely wipes data to ICO standards on all hardware (include photocopiers).
- ☐ Ensure all computers are 'on the network' or synchronised with it regularly, so kept up to date with protection software (anti-virus etc.,) so data is not put at risk.
- ☐ If staff are storing sensitive documents or photographs on the school network, ensure they are in folders in an area restricted to relevant staff only.
- ☐ Ensure that all devices (laptops, USB keys, external hard drives) are actively encrypted if they will be used for storing sensitive data.
- ☐ Ensure back-up is daily and stored in encrypted format. If you use physical tapes, ensure they are stored in a secure, fire-proof safe. Periodically, check back-ups are correctly working. Preferably, use remote, secure back-up, such as LGfL GridStore, for disaster recovery.
- ☐ Set-up auto-lock after 'X' minutes on relevant devices to secure them if they are left idle.
- ☐ Allocate OTP (one time password) tags to staff sending sensitive data across London so all exchange has 'two-factor' data security applied (i.e. username, password, and OTP PIN number.)
- ☐ Use LGfL's USO-FX2, Egress or similar approved system to exchange sensitive data and documents across London schools, e.g. for sending references or documents about named children.
- ☐ Enforce regular password changes where possible. This is essential for systems that contain personal information, e.g. your MIS. (Normal recommendation is every 90 days.)
- ☐ Use recommended email, online platforms or portals and remote access to school or web hosted resources, (i.e. ones that use SSL or IPSec encryption).