Slough and East Berkshire C. of E.
Multi Academy Trust

Data Protection and Security Policy

Owner:	Chris Spencer
Qualified by:	SEBMAT Directors
Date Ratified:	18 March 2019
Date Policy to be reviewed:	18 March 2020

Slough and East Berkshire C. of E.
Multi Academy Trust

Data Protection and IT Security Policy

SEBMAT is committed to compliance with the Data Protection Regulation Act 2018. This policy sets out how we handle the personal data of our pupils, employees, parents and third parties and the precautions we take in order to protect this data. All employees are required to familiarize themselves with the content of this policy and adhere with the provisions set out in it. Failure to comply with this policy is considered an offence which may result in disciplinary action, according to each individual school's disciplinary policy.

Data Protection Regulations Act (2018)

The General Data Protection Regulation 2018 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

Key Definitions

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data subject – any living individual who is the subject of personal data held by an organisation.

Personal data breach **–** a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory

authority and where the breach is likely to adversely affects the rights and freedoms of the of the data subject

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child - Although, in the UK a child is considered to be anyone aged under 18, if you are relying on consent as your lawful basis for processing, in the UK the child may provide their own consent when they are aged 13 or over. If the child is under 13, any consent required will need to be obtained from the parent or custodian.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Data Protection Impact Assessment (DPIAs) – DPIA's are a tool used to identify risks in data processing activities with a view to reducing them.

SEBMAT adheres to the key principles of GDPR when processing personal data, as detailed below.

1. Personal data must be processed lawfully, fairly and in a transparent manner;
2. Personal data must be collected only for specified, explicit and legitimate purposes;
3. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
4. Personal data must be accurate and, where necessary, kept up to date;
5. Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed; and
6. Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

In order to achieve this SEBMAT has implemented the following policies and processes which must be adhered to at all times.

Information Asset Register

SEBMAT and its individual schools have established a data inventory and data flow process as part of its approach to address risks throughout its GDPR compliance project. The Information Asset register determines

1. The data held by the school
2. Who has access to the data and how access is controlled
3. The content and purpose of data
4. Who this data is shared with

5. Legal basis for lawful processing
6. Details of consent where needed
7. Data retention periods and schedules
8. Third party details of people we share data with
9. Data Protection Impact Assessments (DPIA)

The DATA MANAGER (*where a contact is highlighted the relevant contact for each organisation can be found in the index on page 13)*) is responsible for the maintenance of this register and this will be reviewed on a regular basis by the Data Protection Officer (DPO).

Sharing data with Third Parties

SEBMAT will not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. These include–

1. The third party requires the information in order to carry out the contracted service.
2. Sharing the data complies with the published privacy notice and if required, consent is obtained.
3. The transfer complies with any applicable cross-border transfer restrictions
4. The third party has signed a non-disclosure data processing agreement.

Data Subject Rights and Requests

All employees must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends etc. Employees should exercise caution when asked to disclose personal data on an individual. Data Subject Access Requests must be actioned in line with SEBMAT's data subject request procedures. Please see the *Data Subject Request procedures* for more detail at Appendix 3.

Training

The trust will ensure that all employees who handle data have undergone adequate training to enable them to comply with privacy laws and this training will be refreshed at least annually. All new starters will also undergo data protection and IT security training. The schools will also ensure that after the termination of employment, employees and contractors are debriefed on their post-employment confidentiality responsibilities.

Employees should also familiarise themselves with our *privacy notice (*Appendix 1*)* on https://www.sebmat.com/policies-information/other (or via each school website) for more information on how we handle data.

Data Protection Officer (DPO)

Our Data Protection Officer (DPO) is responsible for monitoring internal compliance, informing and advising on data protection obligations, providing advice regarding DPIAs and acting as a contact point for data subjects and the supervisory authorities.

If employees have any questions about the operation of this policy, the GDPR or any concerns about the protection of data within the organisation, please contact the DPO –

DPO: Torix Managed Services

Address: 11a Wessex Road Ind Est, Bourne End, SL8 5DT

Telephone: 01628 914914

Email: SEBMAT-DPO@torix.co.uk

In the event of a data breach/suspected data breach, employees should contact the DPO **immediately**.

For more information on this, please see the *data breach procedure* (Appendix 2)

IT SECURITY POLICY

SEBMAT has taken many steps to ensure the security of our IT systems and protect the data within it. The Director of IT is responsible for the management of our IT security and we have implemented various processes to ensure that a high level of security is maintained. All IT systems are secured using up to date AV and Malware, security and critical patches are installed within 14 days of release, a perimeter firewall is running at all sites.

We ask employees to ensure that when dealing with sensitive or confidential information they ensure that it is secured and stored appropriately. If employees are unsure on the classification of data, how and where it should be stored then please check with the Data Manager.

User Access

In the case of new employees, any data access requirements must be detailed by the HR Manager and sent to the IT Helpdesk as part of a new user set up. No accounts are to be set up with more access rights than necessary for the position. For more information on this matter, please refer to the *joiner/leaver process for each school.*

Any changes in access rights must be approved in writing by a member of the SLT.

A users account and access rights will be deleted immediately after an employee has left. Their data will have previously been archived to a folder only accessible to a member of the SLT. The email account will be retained for 30 days (subject to review) with the password changed and mail forwarded to a relevant member of staff.

To ensure user access is not breached, all computers and electronic devices should be locked when not in use. Employees must immediately inform IT Helpdesk of any security concerns relating to IT systems which could or has led to a data breach.

Any other technical problems that could compromise data (such as hardware errors) should be reported to the IT Helpdesk.

Refer to Appendix 3 for all data subject request procedures and relevant forms.

Network

The security of our networks is of utmost importance and SEBMAT have taken the following steps to maintain this.

1. Network passwords are always changed from the default upon initial configuration.
2. Passwords on all routers or hardware firewall devices are at least 8 characters in length and in line with the password guidelines (Appendix 4)
3. The password on the router or switch is kept in a secure encrypted location.
4. Firmware will be updated on network equipment where vulnerabilities and threats have been identified as part of our regular network equipment and security scans.

Data Protection and IT Security Policy

We ask that employees take the following steps in order to help us maintain our network security

1. Any devices not commissioned by the school/trust should not access the internal network and use the guest network only.
2. The IT Department will endeavour to maintain appropriate filtering methods, but if employees come across any unsuitable sites, this should be reported to IT Helpdesk immediately.
3. Employees should not attempt to gain access to restricted areas of the network or to any password protected information unless they are specifically authorised to do so.
4. Misuse of the computer system may result in disciplinary action. If employees are unsure if actions may constitute misuse then please check with Director of IT before proceeding.
5. Employees are forbidden from accessing, from the school's system, any web page or files which, on the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. While it may be legal in the UK, it may be in sufficient bad taste to fall within this prohibition. Employees must not use the school network to access chat rooms or internet message boards, except those approved by Headteachers in each school. Anyone found accessing inappropriate, offensive or distasteful content on the internet will be open to disciplinary action, up to and including dismissal.

Monitoring

1. The contents of our IT resources and communication systems are SEBMAT's property. Therefore, employees should have no expectation of privacy in any message, files, data, social media post or any other kind of information or communication transmitted to, received, printed from or stored or recorded in our electronic information and comms systems.
2. SEBMAT reserves the right to monitor, intercept and review, without further notice, employees' activities using our IT resources and communications systems, including but not limited to social media posting and activities, to ensure that out rules are being complied with and for legitimate business purposes. Employees consent to such monitoring by acknowledgement of this policy.
3. The school/trust may store copies of such data or communications for a period of time after they are created and may delete such copies from time to time without notice.

Hardware and Software

The purpose of this policy is to standardise and define the usage and setup of hardware and software within SEBMAT. A set of standards have been implemented to "harden" the equipment giving it greater protection from cyber-attack.

Hardware

1. Before purchases are made, all IT systems are assessed by the Director of IT and deemed suitable for compliance with the trust's security requirements.
2. It is the trust's policy to always run data protection impact assessments prior to implementing changes to hardware that may have an impact on the security of our

information systems.

3. All School hardware, computers and mobile devices are to be logged in the asset register which identifies as a minimum, the make, model and location of the item and the named owner (where possible).
4. All employees are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone else, other than in accordance with this policy.
5. Before being commissioned all hardware is to have default passwords changed. This includes ensuring that laptop/desktop computer start up passwords are enabled and that no automatic functions are enabled which trigger actions which can create a security vulnerability, such as auto-play functionality.
6. No hardware other than that commissioned or authorised by the school/trust to be used within the organisation for any purpose without the express permission of the Headteacher or Director of IT.

Software

1. Only authorized software is permitted on the organisation's equipment. Any additional must be approved by a member of the SLT and IT Department.
2. It is the school's policy to always run data protection impact assessments prior to implementing changes to software that may have an impact on the security of our information systems.
3. Specific version upgrades are to be approved by the IT Department.
4. No computer can be used within the business without up to date Anti-Virus and Malware software.
5. Any specific software and/or functions required for work purposes not on the standard list must be approved by a member of the SLT and IT Department.
6. If employees receive an email, they suspect to be Phishing it must not be opened. Please contact the IT helpdesk who will advise how to proceed.
7. If employees detect a virus on any IT equipment, this must be reported to the IT helpdesk immediately.

Data storage

1. No external data storage (USB, CD, DVD, mobile device etc) is permitted without encryption and virus scanning. All employees should also obtain approval from the Director of IT before attaching the device to the network.
2. As soon as data has been transferred from an external device to the school's network, this data must be deleted from the device as soon as possible.
3. All electronic data is automatically backed up at the end of every day.
4. Employees should not take any confidential/sensitive information home without the permission of a member of the SLT. If permission is granted then the technical and practical measures taken in the workplace should also be taken for remote working to maintain the continued security of that information. (i.e., hardcopies kept secure where visitors cannot see them, confidential material should be marked as such).

Email

1. Caution should be taken when sending emails to ensure that information is being sent to the correct person, especially where email addresses auto complete.
2. Employees should be sure to mark all confidential emails as such and circulate the email only to those who need to know this information.
3. Employees should be cautious when opening emails from unknown senders. Do not open attachments or click on links if unsure of their safety. The IT Helpdesk should be informed of any suspected phishing emails, or suspected viruses etc.
4. Email messages should be written as professionally as a letter. Always be concise and direct the email only to the relevant individuals who need the information.
5. Employees should remember that emails can be the subject of legal action for example, in breach of contracts, confidentiality, harassment etc against fellow employees and the school. Therefore, please take care with the content of email messages, as incorrect or improper statements can give rise to personal liability of employees and to liability of the school in the same way as the content of letters.
6. Employees must not agree to terms, enter into contractual commitments or make representations by email unless authority has been obtained by a member of the SLT.
7. Employees who receive an email which has been wrongly delivered should return it to the sender of the message. If the email contains confidential information or inappropriate material it should NOT be disclosed or forwarded to anyone or used in any way. A member of the SLT must be informed as soon as possible.
8. Please be mindful that the school reserves the right to access and read any emails sent over the school network and email system and may recover emails, even after they have been deleted.

SOCIAL MEDIA POLICY

This policy applies to all SEBMAT employees, regardless of their employment status.

Employees are permitted to use Social Media such as Facebook, Linked In, etc. The trust has put in place certain controls to minimise the risks to the school's reputations as well as our confidential and proprietary information.

This policy applies to all forms of social media and internet posting. It also applies to the use of social media for both work AND personal purposes both inside and out of working hours.

1. Social Media must not be used to defame or disparage the trust, school, its employees, pupils, parents, stakeholders or third parties. (Current, past or prospective)
2. Employees must not harass, bully or discriminate against fellow employees, pupils, parents, stakeholders or third parties. (Current, past or prospective) or say anything they may find offensive, including discriminatory comments, insults or obscenity.
3. Employees must not share any personal information about fellow employees, pupils, parents, stakeholders or third parties, (Current, past or prospective)
4. If employees choose to disclose their affiliation with the trust/school as an employee (current past or perspective), they must also state that their views do not represent those of the schools. Even if employees do so, they must still refrain from posting about any confidential or sensitive school related topics.
5. Employees must ensure that their profile and any content posted are consistent with the professional image they are required to present to colleagues, pupils and parents.
6. Employees must not breach any laws or ethical standards
7. Employees must not provide references for other individuals on networking sites as this may be attributed to the school.
8. Employees should not use their work email to sign up to personal social media sites.
9. If employees are contacted for comments about the school for publication anywhere, including any social media outlet, the query must be directed to a member of the SLT and must not be responded to without prior approval.
10. Employees must not use the trust's logos, slogans or any intellectual property without prior consent from a member of the SLT.

If employees are unsure if a post is in breach of this policy, please check with a member of the SLT before posting. Social media content that is in breach of this policy should also be reported to a member of the SLT.

When posting on the school's social media account employees must

1. Ensure that permission from the child's parent has been sought to use photos on social media. This information can be found in SIMS
2. Ensure that there is no identifying information relating to the child. (E.g. their full name is not showing on a piece of work)

3. The post must be a positive and relevant post relating to the children, the good work of employees, the school or any other achievements.
4. All photos taken for the purpose of social media/school use on personal devices must be deleted as soon as they are uploaded onto a device belonging to the school.

PASSWORD POLICY

The purpose of this policy is to establish the standard for strong passwords, the protection of those passwords and the frequency of change.

Password Creation

1. All user-level and system-level passwords must conform to the *Password Guidelines (Appendix 4)* . This is enforced on all systems that we are able to. The Director of IT is responsible for administering this.
2. Users must not use the same password for School accounts as for other non-School access (for example, personal ISP account, option trading, benefits, and so on).
3. Where possible, users must not use the same password for various School access needs.
4. User accounts that have system-level privileges must have a unique password from all other accounts held by that user.

There are many actions that employees can take to help ensure password protection and in doing so, helping secure the data that SEBMAT is responsible for. We ask that all employees take the following steps when dealing with passwords to school apps/systems.

Password Protection

1. Passwords must not be shared with anyone. All passwords are to be treated as sensitive,
2. Passwords must not be inserted into email messages or other forms of electronic communication.
3. Do not share School passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on holiday/annual leave and family members.
4. If employees **must** share a password with a member of the leadership team (when out of the office/sick etc) the IT Helpdesk must be notified to get this password changed ASAP.
5. Any employees found to be accessing IT systems, using another staff member log in details will be liable to disciplinary action, up to and including dismissal for gross misconduct.
6. Do not reveal a password on questionnaires or security forms.
7. Do not hint at the format of a password (for example, "my family name") anywhere.
8. Employees must not leave applications or workstations logged in when leaving their desk/office in order to prevent unauthorised access. If workstations are left logged in and this results in a breach – the individual employee may be held liable and may result in disciplinary action.

9. Do not write passwords down and store them anywhere within the office/classroom. Do not store passwords in a file on a computer system or mobile devices (phone, tablet,) without encryption.
10. Any user suspecting that his/her password may have been compromised must report the incident to the DPO and IT Helpdesk and change all passwords

External contractors and visitors

1. Wi-Fi network passwords should not be given to visitors. If it is given in error, it must be changed immediately.
2. External contractors needing access which requires passwords must sign up to and adhere to all the IT policies/NDA which regular permanent employees sign up to.

PHYSICAL SECURITY POLICY

It is not just cyber security that SEBMAT need to be aware of in regards to data protection, it is also the physical security of data. This is not exclusive to access of computers and networks.

Paper records and documents containing personal information, sensitive personal information and confidential information must be positioned in a way to avoid them being viewed by others (i.e. not to leave these lying on your desk whilst going to lunch etc) and all such documents must be locked away in a secure cupboard at the end of use. The DATA MANAGER is the only person with access to these locked cupboards, should you need to access any information.

All unattended computers and IT equipment must be locked and only accessible by entering a unique username and password.

The physical security of the building is of high importance and is reviewed regularly. However, if you find any concerns of liabilities to this security, please report this to Headteacher.

Such measures are determined and reviewed according to each schools' capabilities.

Data Protection and IT Security Policy

Organisation Contacts

School	Data Owner	Data Manager
SEBMAT	Chris Spencer	Clare McAleer
Slough and Eton C of E Business and Enterprise College	Peter Collins	Deborah England
Colnbrook C of E Primary School	Susan Marsh	Beverley Richards
Eton Porny C of E Fist School	Katherine Russell	Kate Hilton
Lynch Hill School Primary Academy	Gillian Coffey	Michele Cawte
Lynch Hill Enterprise Academy	Chris Thomas	Kay MacKenzie

Related policies and procedures–

Appendix 1 Privacy Notice

Appendix 2 Data Breach Procedure

Appendix 3 Data Subject Request Procedures and relevant forms (Access Request; Change Requests; Deletion and Restricting of Processing Requests; Portability Requests)

Appendix 4 Password Guidelines

Please note: Failure to comply with the above guidelines, and other policies laid out by SEBMAT may lead to disciplinary action.

I confirm that I have read and understood the above policy -

Employee Name _____

Signature _____

Position _____

Date _____

Appendix 1

PRIVACY NOTICE

Personal data

Under the EU's General Data Protection Regulation (GDPR) personal data is defined as:

> "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

How we use your information

SEBMAT is the "data controller" for the purposes of data protection law. This privacy notice tells you how we, SEBMAT, will collect and use your personal data for:

- support our pupils' learning
- monitor and report on their progress
- protect pupil welfare
- provide appropriate pastoral care
- assess the quality of our services
- administer admissions waiting lists
- comply with the law regarding data sharing

Why does SEBMAT need to collect and store personal data?

SEBMAT collects data to comply with legal requirements or in order for us to provide you with a service. We need to collect personal data for contact details of pupils and parents, biometric data for paying for school lunches, national curriculum assessment results, attendance information, any exclusion information, CCTV footage, where pupils go after they leave us and personal characteristics such as ethnic group, any special educational needs pupils may have as well as relevant medical information. In any event, we are committed to ensuring that the information we collect and use is appropriate for this purpose, and does not constitute an invasion of your privacy.

We seek pupil/parental consent before taking photographs or filming children. These photographs/films are used as part of their individual activity tracking, forming part of our educational process and will only be shared with pupils, school staff and the child's parents or legal guardians.

We obtain consent further consent from the pupil/parents or legal guardians to use photos for school promotional purposes including but not limited to school social media accounts, the school prospectus, website or pictures on walls as part of the application process.

When we collect personal data that is does not hold a legitimate interest or a legal requirement, we will contact the pupil/parent for consent.

Will SEBMAT share my personal data with anyone else?

We may pass your personal data on to third-party service providers contracted to SEBMAT in the course of dealing with you as well as schools that pupils may move to, the local authority, youth support services and the department for education. Any third parties that we may share your data with are obliged to keep your details securely, and to use them only to fulfil the service they provide you on our behalf. When they no longer need your data to fulfil this service, they will dispose of the details in line with SEBMAT's procedures. If we wish to pass your sensitive personal data onto a third party we will only do so once we have obtained your consent, unless we are legally required to do otherwise.

How will SEBMAT use the personal data it collects about me?

SEBMAT will process (collect, store and use) the information you provide in a manner compatible with the EU's General Data Protection Regulation (GDPR). We will endeavor to keep your information accurate and up to date, and not keep it for longer than is necessary. SEBMAT is required to retain information in accordance with the law. How long certain kinds of personal data should be kept may also be governed by education-sector specific requirements and agreed practices. Personal data may be held in addition to these periods depending on individual business needs. Further information on data retention periods can be supplied on request.

Under what circumstances will SEBMAT contact me?

Our aim is not to be intrusive, and we undertake not to ask irrelevant or unnecessary questions. Moreover, the information you provide will be subject to rigorous measures and procedures to minimise the risk of unauthorised access or disclosure.

Can I find out the personal data that the organisation holds about me?

SEBMAT, at your request, can confirm what information we hold about you and how it is processed. If SEBMAT does hold personal data about you, you can request the following information:

- Identity and the contact details of the person or organisation that has determined how and why to process your data. In some cases, this will be a representative in the EU.
- Contact details of the data protection officer, where applicable.
- The purpose of the processing as well as the legal basis for processing.
- If the processing is based on the legitimate interests of SEBMAT or a third party, information about those interests.
- The categories of personal data collected, stored and processed.
- Recipient(s) or categories of recipients that the data is/will be disclosed to.
- If we intend to transfer the personal data to another country or international organisation, information about how we ensure this is done securely. The EU has approved sending personal data to some countries because they meet a minimum standard of data protection. In other cases, we will ensure there are specific measures in place to secure your information.
- How long the data will be stored.
- Details of your rights to correct, erase, restrict or object to such processing.
- Information about your right to withdraw consent at any time.
- How to lodge a complaint with the supervisory authority.

- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether you are obliged to provide the personal data and the possible consequences of failing to provide such data.
- The source of personal data if it wasn't collected directly from you.
- Any details and information of automated decision making, such as profiling, and any meaningful information about the logic involved, as well as the significance and expected consequences of such processing.

What forms of ID will I need to provide in order to access this?

In order to receive this information, you can contact our Data Protection Officer about raising a data subject access request, change requests, portability requests or the deletion and restriction of processing request. In order to do so, you will need to provide some proof of identification. SEBMAT accepts the following forms of ID when information on your personal data is requested:
Passport, driving licence, birth certificate. (If photo identification not available then you will also need to provide a utility bill from the last 3 months).

Contact details of the Data Protection Officer:

If you have any enquiries or require assistance with data protection matters, please feel free to contact out DPO. Contact details below:

Name:	Torix DPO Services
E-mail:	SEBMAT-DPO@torix.co.uk
Address:	Torix, Unit 11a Wessex Road Industrial Estate, Bourne End, SL8 5DT
Phone:	01628 914914

Appendix 2

Data Breach Procedure

1. Scope

This procedure applies in the event of a personal data breach under Article 33 of the GDPR – *Notification of a personal data breach to the supervisory authority* – and Article 34 – *Communication of a personal data breach to the data subject*.

2. Responsibility

2.1 All users (whether Employees/Staff, contractors or temporary Employees/Staff and third-party users) of SEBMAT are required to be aware of, and to follow this procedure in the event of a personal data breach.

2.2 All Employees/Staff, contractors or temporary personnel are responsible for reporting any personal data breach to the Data Protection Officer.

3. Procedure – Breach notification data protection officer

3.1 SEBMAT reports any personal data breach or security incident to the data protection officer without undue delay. These details are recorded in the Internal Breach Register. SEBMAT provides the DPO with all of the details of the breach.

3.2 The breach notification is made by email to the details below
In the event of a data breach – please collate as much information as possible and notify your DPO on details below.

Name:	Torix DPO Services
E-mail:	SEBMAT-DPO @torix.co.uk
Address:	Torix, Unit 11a Wessex Road Industrial Estate, Bourne End, SL8 5DT
Phone:	01628 914914

3.3 A confirmation of receipt of this will be sent to the school and the information is recorded by email.

4. Procedure – Breach notification data controller to supervisory authority

4.1 DPO determines if the supervisory authority need to be notified in the event of a breach.

4.2 DPO assesses whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach, by conducting a data protection impact assessment.

4.3 If a risk to data subject(s) is likely, DPO reports the personal data breach to the supervisory authority (ICO) without undue delay, and not later than 72 hours.

4.4 If the data breach notification to the supervisory authority is not made within 72 hours, the DPO submits it electronically with a justification for the delay.

4.5 If it is not possible to provide all of the necessary information at the same time DPO will provide the information in phases without undue further delay.

4.6 The following information needs to be provided to the supervisory authority

- 4.6.1 A description of the nature of the breach.
- 4.6.2 The categories of personal data affected.
- 4.6.3 Approximate number of data subjects affected.
- 4.6.4 Approximate number of personal data records affected.
- 4.6.5 Name and contact details of the Data Protection Officer.
- 4.6.6 Consequences of the breach.
- 4.6.7 Any measures taken to address the breach.
- 4.6.8 Any information relating to the data breach.

4.7 The Data Protection Officer notifies the supervisory authority (ICO). Contact details for the supervisory authority are recorded below.

4.8 In the event the supervisory authority assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register.

4.9 The breach notification is made by email

4.10 A confirmation of receipt of this information is recorded by email.

5. Procedure – Breach notification data controller to data subject

5.1 If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, SEBMAT notifies those/the data subjects affected immediately

5.2 The notification to the data subject describes the breach in clear and plain language, in addition to information specified in clause 4.6 above.

5.3 SEBMAT takes measures to render the personal data unusable to any person who is not authorised to access it using encryption.

5.4 SEBMAT takes subsequent measures to ensure that any risks to the rights and freedoms of the data subjects are no longer likely to occur by securing the liability that caused the breach.

5.5 If the breach affects a high volume of data subjects and personal data records, SEBMAT makes a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder SEBMAT's ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure informs those affected in an equally effective manner.

5.6 If SEBMAT has not notified the data subject(s), and the supervisory authority considers the likelihood of a data breach will result in high risk, SEBMAT will then communicate the data breach to the data subject by email/phone call.

5.7 SEBMAT documents any personal data breach(es), incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.

A review of the breach should then be carried out to see if changes need to be implemented to procedures in order to avoid a repetition of breach.

Appendix 3

Data Subject Request Procedures

Introduction

This document provides details of processes that should be followed for each of the following data subject requests – Access, Portability, Change, Deletion, Suspension of Processing

Access Request

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully.

You have 28 days to comply with the request from the date of receipt. Please bear in mind school holidays are not exempt from this time period.

See Access Request form

ACCESS REQUEST PROCESS

1) The request should be managed by the *Data Manager*.

2) Add the request into the Data Subject request log including delivery date within 28 days of the initial request.

3) Confirm with the requester exactly what information they want by asking them to complete Access request form.

4) Obtain signed declaration from the data subject \ the person requesting on behalf of the data subject

5) Create a directory in a secure location to store the extracted information and records of correspondence relating to the request.

6) Do you have enough information to be sure of the requester's identity?

7) Do you need more information from the requester to find what they want?

8) Are you charging a fee?
    a. Is this the 1st request?
    b. Is the request reasonable \ not excessive?

(when to charge - see link to ICO - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/a fee add link from ICO)

9) Find relevant information:
    a. Identify information held on data subject using the "Information Asset Register".
        i. The register is split into sections for Employee Data, Client Data, Supplier Data.

10) Screen the information
    a. Not all personal information may be liable for disclosure so blank out or exclude information that should not be disclosed.
    b. Does it include information about other people?
        i. You will not have to supply the information unless the other people mentioned have given their consent for the disclosure, or it is reasonable to supply the information without their consent.

11) Copy Data held electronically to a separate location to the original copy

12) Scan hard copies and save to the new location. A copy of the redacted data sent to the data subject, should be stored.

13) Provide to the data subject \ requesting party via agreed means in a permanent form where possible.

14) Update the Data Subject Request Record accordingly.

Appendix 3.1

Access Request

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. Access request will be actioned within 28 days. Please bear in mind school holidays are not exempt from this time period.

DATA SUBJECT DETAILS:

Title	Mr ☐	Mrs ☐	Miss ☐	Ms ☐	Other: ☐
Surname					
First name(s)					
Current address					
Telephone number:					
Landline					
Mobile					
Email address					
Details of identification provided to confirm identity:	Passport ☐, Driving licence ☐, Birth certificate ☐, Utility bill (from last 3 months) ☐, Bank statement (from last 3 months) ☐				

DETAILS OF PERSON REQUESTING THE INFORMATION (if not the data subject):

Are you acting on behalf of the data subject with their *[written]* or other legal authority?	Yes ☐ No ☐				
If 'Yes' please state your relationship with the data subject (e.g. parent, legal guardian or solicitor)					
Please enclose proof that you are legally authorised to obtain this information.					
Title	Mr ☐	Mrs ☐	Miss ☐	Ms ☐	Other: ☐
Surname					
First name(s)					
Current address					
Telephone number:					
Landline					
Mobile					
Email address					
Details of identification provided to confirm identity:	Passport ☐, Driving licence ☐, Birth certificate ☐, Utility bill (from last 3 months) ☐, Bank statement (from last 3 months) ☐				

REQUEST DETAILS

Details of information requested	

DECLARATION

I, _____, hereby request that SEBMAT provide me with the data requested about the data subject identified above.

Appendix 3.2

Change Requests

The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. Requests will be processed within 28 days. Please bear in mind school holidays are not exempt from this time period. In certain circumstances we may refuse a request for rectification.

DATA SUBJECT DETAILS:

Title	Mr ☐	Mrs ☐	Miss ☐	Ms ☐	Other: ☐
Surname					
First name(s)					
Telephone number:					
Landline					
Mobile					
Email address					
Details of identification provided to confirm identity:	Passport ☐, Driving licence ☐, Birth certificate ☐, Utility bill (from last 3 months) ☐, Bank statement (from last 3 months) ☐				

REQUEST DETAILS:

Information Affected	*e.g. Home Address, E-mail Address, Phone Number*
Request Details	*e.g. change of address*

DETAILS OF PERSON REQUESTING THE INFORMATION (if not the data subject):

Are you acting on behalf of the data subject with their *[written]* or other legal authority?	Yes ☐ No ☐

If 'Yes' please state your relationship with the data subject (e.g. parent, legal guardian or solicitor)					
Please enclose proof that you are legally authorised to obtain this information.					
Title	Mr ☐	Mrs ☐	Miss ☐	Ms ☐	Other: ☐
Surname					
First name(s)					
Current address					
Telephone number:					
Landline					
Mobile					
Email address					
Details of identification provided to confirm identity:	Passport ☐, Driving licence ☐, Birth certificate ☐, Utility bill (from last 3 months) ☐, Bank statement (from last 3 months) ☐				

Appendix 3.3

Deletion and Restriction of Processing Requests

The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. We will attempt to action this within 28 days. Please bear in mind school holidays are not exempt from this time period.

The right is not absolute and only applies in certain circumstances i.e. if the information is held for legal or contractual reasons. Information held based on legitimate interests or consent should be deleted.

DATA SUBJECT DETAILS:

Title	Mr ☐	Mrs ☐	Miss ☐	Ms ☐	Other: ☐
Surname					
First name(s)					
Telephone number:					
Landline					
Mobile					
Email address					
Details of identification provided to confirm identity:	Passport ☐, Driving licence ☐, Birth certificate ☐, Utility bill (from last 3 months) ☐, Bank statement (from last 3 months) ☐				

REQUEST DETAILS:

Request Type	Deletion ☐	Restriction of Processing ☐
Information Affected	*e.g. Contact Details*	
Request Details	*e.g. Remove client from marketing database*	

DETAILS OF PERSON REQUESTING THE INFORMATION (if not the data subject):

Are you acting on behalf of the data subject with their *[written]* or other legal authority?			Yes ☐ No ☐		
If 'Yes' please state your relationship with the data subject (e.g. parent, legal guardian or solicitor)					
Please enclose proof that you are legally authorised to obtain this information.					
Title	Mr ☐	Mrs ☐	Miss ☐	Ms ☐	Other: ☐
Surname					
First name(s)					
Current address					
Telephone number:					
Landline					
Mobile					
Email address					
Details of identification provided to confirm identity:	Passport ☐, Driving licence ☐, Birth certificate ☐, Utility bill (from last 3 months) ☐, Bank statement (from last 3 months) ☐				

DECLARATION

I, _____, hereby request that SEBMAT delete any data held about the data subject identified above.

Appendix 3.4

Portability Requests

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits. The right only applies to information an individual has provided to a controller.

We will comply with request within 28 days. Please bear in mind school holidays are not exempt from this time period.

DATA SUBJECT DETAILS:

Title	Mr ☐	Mrs ☐	Miss ☐	Ms ☐	Other: ☐
Surname					
First name(s)					
Telephone number:					
Landline					
Mobile					
Email address					
Details of identification provided to confirm identity:	Passport ☐, Driving licence ☐, Birth certificate ☐, Utility bill (from last 3 months) ☐, Bank statement (from last 3 months) ☐				

REQUEST DETAILS:

Information Affected	*e.g. Home Address, E-mail Address, Phone Number*
Format data required in:	*Excel, CSV etc.*
How will the data be transmitted?	*Must be transmitted securely*

Appendix 4

Password Guidelines

The purpose of these guidelines is to provide best practices for the creation of strong passwords

All passwords should meet or exceed the following guidelines

Strong passwords have the following characteristics:

- Contain at least eight alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/).

Poor, or weak, passwords have the following characteristics:

- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of “Welcome123” “Password123” “Changeme123”

You should **never** write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.