Data Protection Policy

Review Date: May 2024
Review by: Pastoral, Safeguarding, Wellbeing Committee
Final Approval: Pastoral, Safeguarding, Wellbeing Committee

Academy Context
The Core Values of the Academy which relate specifically to this policy state that we are working together to form relationships based on

- Truth - everyone is required to be honest and to communicate in a positive manner
- Responsibility - everyone is expected to understand the consequences of their actions
- Justice - everyone is entitled to be treated fairly and to promote the self-esteem of others

Such values contribute to our common purpose of "Striving for high quality education with a strong Christian ethos", and underpin, data practices within the Academy.

Data Protection
Any personal data processed in the delivery of this policy will be processed in accordance with the Academy Data Protection policy.

Policy Contents

1. Policy statement

1.1 Bishop Stopford Academy collects and uses personal information about **staff,** students, parents and other individuals who come into contact with the Academy. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the Academy complies with its statutory obligations. During the course of our activities as an Academy we will collect, store and **process personal data** about our students, **staff,** parents and other stakeholders. This makes us a **data controller** in relation to that **personal data**.

1.2 We are committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.

1.3 The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.

1.4 All members of our **staff** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

1.5 Everyone has rights regarding the way personal data is handled including the right of access.

2 About this policy

2.1 This policy meets the requirement of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (2018). It is based on guidance published by the Information Commissioner's Office (ICO) on the data protection legislation and the ICOs Code of Practice for Subject Access Requests. This Policy also reflects the ICO's Code of Practice for Surveillance cameras and Personal Information.

2.2 The types of **personal data** that we may be required to handle include information about students, parents, **staff**, governors and other stakeholders that we deal with. The **personal data** which we hold is subject to certain legal safeguards specified in **UK GDPR** and the Data Protection Act (2018),

2.3 This policy and any other documents referred to within t set out the basis on which we will **process** any **personal data** we collect from **data subjects**, or is provided to us by **data subjects** or from other sources, or is otherwise generated in the course of our day to day activities.

2.4 This policy applies to all staff and volunteers employed by or working on behalf of the Academy and to external organisations or individuals working on our behalf.

2.5 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.6 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process **personal data**.

3 Definition of data protection terms

3.1 All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in Annex 1 to this policy.

4 Roles and Responsibilities

4.1 Trustees and the Governing Body

4.1.1 The Trustees and governing body have overall responsibility for ensuring that the Academy complies with all relevant data protection obligations.

4.2 Data Protection Officer

4.2.1 As an Academy, we are required to appoint a Data Protection Officer ("DPO"). The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. (see Annex 2 for contact details)

4.2.2 The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

4.2.3 The DPO is also the central point of contact for all **data subjects** and others in relation to matters of data protection.

5 Data protection principles

5.1 Anyone **processing personal data** must comply with the data protection principles. These provide that **personal data** must be:

5.1.1 **Processed** fairly and lawfully and transparently in relation to the **data subject**;

5.1.2 **Processed** for specified, lawful purposes and in a way which is not incompatible with those purposes;

5.1.3 Adequate, relevant and not excessive for the purpose;

5.1.4 Accurate and kept up to date;

5.1.5 Not kept for any longer than is necessary for the purpose; and

5.1.6 **Processed** securely using appropriate technical and organisational measures.

These fundamental principles are further strengthened by the addition of the "Accountability Principle", which places a duty on data controllers and processors to demonstrate their compliance with the Principles

5.2 **Personal Data** must also:

5.2.1 be **processed** in line with **data subjects'** rights; not be transferred to people or organisations situated in third- countries without adequate protection.

5.3 We will comply with these principles in relation to any **processing** of **personal data** by the Academy.

6 Fair and lawful processing

6.1 Data Protection Legislation is not intended to prevent the **processing** of **personal data**, but to ensure that it is done fairly and without adversely affecting the rights of the **data subject**.

6.2 For **personal data** to be **processed** fairly, **data subjects** must be made aware:

6.2.1 that the **personal data** is being **processed**;

6.2.2 why the **personal data** is being **processed**;

6.2.3 what the lawful basis is for that **processing** (see below);

6.2.4 whether the **personal data** will be shared, and if so with whom;

6.2.5 the period for which the **personal data** will be held;

6.2.6 the existence of the **data subject's** rights in relation to the **processing** of that **personal data**; and

6.2.7 the right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

6.3 We will only obtain such **personal data** as is necessary and relevant to the purpose for which it was collected and will not process it further for reasons incompatible with the original purpose for which it was collected.

6.4 For **personal data** to be **processed** lawfully, it must be **processed** on the basis of one or more of the lawful basis set out in the Data Protection Legislation. We will normally **process personal data where** :-

6.4.1 the **processing** is necessary for the performance of a contract between us, or to take steps prior to entering into a contract such as contacting a previous employer for a reference.

6.4.2 the **processing** is necessary to comply with a legal obligation that we are subject to, (e.g. the Education Act 2011)

6.4.3 processing is necessary to protect the vital interest of the individual e.g to protect someone's life

6.4.4 the Academy, as a public authority performs a task **in the public interest,** or in the exercise of our official functions; and,

where none of the above apply then we will seek the consent of the **data subject** to **process** their **personal data.**

6.5 When **special category personal data** is being processed then an additional lawful bases must apply to that processing. We will normally only **process special category personal data** where:

6.5.1 the **processing** is necessary to carry out rights and obligations under employment law purposes, for example in relation to sickness absence, ensuring the health and safety

of employees or complying with discrimination or unfair dismissal laws, etc

6.5.2 the **processing** is necessary to ensure the vital interest of the individual where they are physically or legally incapable of giving consent

6.5.3 the processing is necessary for the purpose of preventative or occupational medicine, for the assessment of a person's working capacity, either on the basis of UK law or in accordance with a contract with a health professional such as an external occupational health provider

6.5.4 the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment

6.5.5 the **processing** is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

6.5.6 the data has been manifestly made public by the data subject

6.5.7 the processing is necessary for archiving purposes in the public interest , scientific or historical research purposes or statistical purposes

6.5.8 if none of the above apply then we will seek the explicit consent of the **data subject** to **process** their **special category personal data**.

6.6 We will inform **data subjects** of the above matters by issuing Privacy Notices at the point of data collection, or as soon as possible thereafter, unless we have already provided this information such as at the time when a student or staff member joins us.
If any **data user** is in doubt as to whether they can use any **personal data** for any purpose then they must contact the DPO before doing so.

Less commonly, information relating to criminal convictions may be used where necessary in relation to legal claims; where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

7 Criminal Convictions

7.1 The Academy may use information relating to criminal convictions where the law allows us to do so. The Academy will hold information about criminal convictions if information about criminal convictions comes to light as a result of recruitment and Disclosure and Barring Service checks, or if any information about criminal convictions becomes apparent during a stakeholder relationship with us.

7.2 Information about criminal convictions and offences will be used to ensure suitability to work for us and for safeguarding purposes.

7.3 Less commonly, information relating to criminal convictions may be used where necessary in relation to legal claims; where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where the information has already been made public

8 Consent

8.1 Where none of the other bases for **processing** set out above apply, then the Academy must seek the consent of the **data subject** before **processing** their **personal data** for a specific purpose

8.2 There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.

8.3 When students and/or staff join the Academy a consent form will be required to be completed in relation to them. For students in Key Stages 3 and 4 this will need to be countersigned by an individual with parental responsibility for that student. Where appropriate third parties may also be required to complete a consent form.

8.4 If consent is required for any other **processing** of **personal data** of any **data subject** then the form of this consent must be:

8.4.1 Freely given - The data subject must have a genuine choice and be able to refuse or withdraw consent

8.4.2 Specified - given for a specific and fully explained processing operation

8.4.3 Informed – the data subject should be provided with all the necessary details of the processing activity in a language and form that can understand

8.4.4 Unambiguous indication of wishes – the data subjects clear affirmative action or

statement must leave no doubt as to their intention to give consent

8.5 Consent given as a condition of employment or other duress or coercion is not valid consent.

8.6 The DPO must always be consulted in relation to any proposed amendments to consent forms.

8.7 A record must always be kept of any consent, including how it was obtained, when and for what purpose.

9 Notifying data subjects

9.1 If we collect **personal data** directly from **data subjects**, we will inform them about:

9.1.1 our identity and contact details as **Data Controller** and those of the DPO;

9.1.2 the purpose or purposes and lawful basis for the processing

9.1.3 the types of third parties, if any, with which we will share or disclose the **personal data**;

9.1.4 whether the **personal data** will be transferred outside UK, and if so the safeguards in place;

9.1.5 the period for which their **personal data** will be stored, by reference to our Retention Policy and Schedule;

9.1.6 the existence of any automated decision making in the **processing** of the **personal data** along with the significance and envisaged consequences of the **processing** and the right to object to such decision making; and

9.1.7 the rights of the **data subject** to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

9.2 Unless we have already informed **data subjects** that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive **personal data** about a **data subject** from other sources, we will provide the **data subject** with the above information as soon as possible, thereafter, informing them of where the **personal data** was obtained.

10 Adequate, relevant and necessary processing

10.1 The principle of data minimisation means that we must only collect and process personal data that is relevant, necessary and adequate to accomplish the purpose for which it is processed

10.2 Data must be suitable and proportionate to achieve the processing purpose

11 Accurate data

11.1 We will ensure that **personal data** we hold is accurate and kept up to date.

11.2 We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

11.3 **Data subjects** have a right to have any inaccurate **personal data** rectified. See further below in relation to the exercise of this right.

12 Storage Limitation

12.1 We will not keep **personal data** longer than is necessary for the purpose or purposes for which they were collected unless required to do so by law.

12.2 We will take all reasonable steps to destroy, or erase from our systems, all **personal data** which is no longer required in accordance with our Data Retention Policy and Schedule.

13 Processing in line with data subjects' rights

13.1 We will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:

13.1.1 request access to the **personal data** we hold about them;

13.1.2 object to the **processing** of their **personal data** in certain circumstances, including the right to object to direct marketing;

13.1.3 have inaccurate or incomplete **personal data** about them rectified

13.1.4 restrict **processing** of their **personal data**, in certain circumstances

13.1.5 have **personal data** we hold about them erased, in certain circumstances

13.1.6 have their **personal data** transferred; and

13.1.7 object to the making of decisions about them by automated means.

The Right of Access to Personal Data

13.2 **Data subjects** may request access to all **personal data** we hold about them. Such requests

will be considered in line with the Academy's Subject Access Request Procedure. This procedure is available on our Academy website or on request to the Academy office.

The Right to Object

13.3 In certain circumstances **data subjects** may raise objections to the **processing of** their **personal data** on the basis of a legitimate interest or data processed for scientific, historical or research purposes provided the processing is not necessary for the performance of a task carried out in the public interest.

13.4 An objection to **processing** does not have to be complied with where the Academy can demonstrate compelling grounds which override the interests, freedoms and rights of the **data subject**.

13.5 Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

13.6 In respect of direct marketing, any objection to **processing** must be complied with.

13.7 The Academy is not however obliged to comply with a request where the **personal data** is required in relation to the establishment, exercise of defence of legal claims or proceedings.

The Right to Rectification

13.8 If a **data subject** informs the Academy that **personal data** held about them by the Academy is inaccurate or incomplete then we will consider a request for rectification. In most cases it will be sufficient of the data subject to simply request rectification of, for example, the spelling of a name, change of address or telephone number

13.9 If, however, requests are linked to legally significant matters such as the data subject's legal identity, requests for rectification will be followed by a request for proof of the alleged inaccuracy prior to rectification.

13.10 If we consider the issue to be too complex to resolve within the time period permitted (one calendar month) then we may extend the response period by a further two months. If this is necessary, then we will inform the **data subject** within one month of their request that this is the case.

13.11 We may determine that any changes proposed by the **data subject** should not be made. If this is the case then we will explain to the **data subject** why this is the case. In those circumstances we will inform the **data subject** of their right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

The Right to Restrict Processing

13.12 **Data subjects** have a right to request "blocking" or suppressing the **processing** of **personal data**. This means that the Academy can continue to hold the **personal data** but not do anything else with it during the period for which that right applies.

13.13 The Academy must restrict the **processing** of **personal data where**:

- 13.13.1 the accuracy of the data is contested and for as long as it takes to verify the accuracy and rectify the data if necessary
- 13.13.2 the Academy is in the process of considering an objection to processing by a **data subject**
- 13.13.3 the **processing** is unlawful, but the **data subject** has asked the Academy not to delete the **personal data**; and
- 13.13.4 the Academy no longer needs the **personal data** but the **data subject** has asked the Academy not to delete the **personal data** because they need it in relation to a legal claim, including any potential claim against the Academy.

13.14 If the Academy has shared the relevant **personal data** with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

13.15 The DPO must be consulted in relation to requests under this right.

The Right to Be Forgotten

13.16 **Data subjects** have a right to have **personal data** about them held by the Academy erased only in the following circumstances:

13.16.1 Where the **personal data** is no longer necessary for the purpose for which it was originally collected and no new lawful purpose exists
13.16.2 When a **data subject** withdraws consent – which will apply only where the Academy is relying on the individuals consent to the **processing** in the first place
13.16.3 When a **data subject** objects to the **processing** and there is no overriding legitimate interest to continue that **processing** – see above in relation to the right to object;
13.16.4 Where the **processing** of the **personal data** is otherwise unlawful;
13.16.5 When it is necessary to erase the **personal data** to comply with a legal obligation

13.17 The Academy is not required to comply with a request by a **data subject** to erase their **personal data** if the **processing** is taking place:
13.17.1 To exercise the right of freedom of expression or information;
13.17.2 To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law
13.17.3 For public health purposes in the public interest;
13.17.4 For archiving purposes in the public interest, research or statistical purposes;
13.17.5 For the establishment of, exercise of, or defence of a legal claim.

13.18 If the Academy has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

13.19 The DPO must be consulted in relation to requests under this right.

Right to Data Portability

13.20 In limited circumstances, a **data subject** has a right to receive their **personal data** in a machine-readable format, and to have this transferred to other organisations.

13.21 This right only applies to data provided to the Data Controller, directly by the data subjectunder contract

13.22 This right only applies to data held electronically

13.23 If such a request is made, then the DPO must be consulted.

14 Data security

14.1 We will take appropriate security measures against unlawful or unauthorised processing of **personal data**, and against the accidental loss of, or damage to, **personal data**.

14.2 We will put in place appropriate operational and technological measures to maintain the security of all **personal data** from the point of collection to the point of destruction. A summary of these are included in Annex 3

14.3 Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

15 Data Protection By Design and Default

15.1 We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:
15.1.1 Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
15.1.2 Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
15.1.3 Completing Data Privacy Impact Assessments where the Academy's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (see section 15 below)
15.1.4 Integrating data protection into internal documents including this policy, any related policies and privacy notices
15.1.5 Regular training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
15.1.6 Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
15.1.7 Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our Academy and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

16 Data Protection Impact Assessments

16.1 The Academy takes data protection very seriously, and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

16.2 In certain circumstances the law requires us to carry out detailed assessments of proposed **processing**. This includes where we intend to use new technologies, which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing** or the way that we intend to do so.

16.3 The Academy will complete an assessment of any such proposed **processing** and has a template document which ensures that all relevant matters are considered.

16.4 The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

17 Disclosure and sharing of personal information

17.1 We may share **personal data** that we hold about **data subjects**, and without their consent, with other organisations. Such organisations include the Department for Education, and Education and Skills Funding Agency "ESFA", Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

17.2 The Academy will inform **data subjects** of any sharing of their **personal data** unless we are not legally required to do so, for example where **personal data** is shared with the police in the investigation of a criminal offence.

17.3 In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy which can be accessed on the Academy website.

17.4 Further detail is provided in our Schedule of Processing Activities.

18 Data Processors

18.1 We contract with various organisations who provide services to the Academy, including:

18.1.1 Payroll providers, HR, legal and health and safety advisors, Caterers, Online Payment Facilities, Student counselling services, Examination Boards, Local Authority e.g. Social Services, Police, Teachers Pension Scheme and the Local Government Pension Scheme, Academy photographer, I.T. Administration systems for managing student and staff data, medical services.

18.2 In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.

18.3 **Personal data** will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Academy. The Academy will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.

18.4 Contracts with **data processors** will comply with Data Protection Legislation and contain explicit obligations on the **data processor** to ensure compliance with the Data Protection Legislation, and compliance with the rights of **Data Subjects**.

19 Images and Videos

19.1 Parents and others attending Academy events are allowed to take photographs and videos of those events for domestic purposes. For example, parents may take video recordings of a

Academy performance involving their child. The Academy does not prohibit this as a matter of policy.

19.2 The Academy does not however agree to any such photographs or videos being used for any other purpose except for domestic use, but acknowledges that such matters are, for the most part, outside of the ability of the Academy to prevent.

19.3 The Academy asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

19.4 As a Academy we want to celebrate the achievements of our students and therefore may want to use images and videos of our students within promotional materials, or for publication in the media such as local, or even national, newspapers covering Academy events or achievements. We will seek the consent of students, and their parents where appropriate, before allowing the use of images or videos of students for such purposes.

19.5 Whenever a student registers at the Academy they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that student by the Academy. We will not use images or videos of students for any purpose where we do not have consent.

20 CCTV

20.1 The Academy operates a CCTV system and we will adhere to the ICO's code of practice for the use of CCTV

20.2 The purpose of the system is to prevent crime and promote security and public safety. If, in the event of viewing CCTV for the specified purpose, a disciplinary action is observed, the CCTV can be used for the purpose of a disciplinary investigation.

20.3 We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

20.4 Please refer to the Academy CCTV Policy for further information on this

21 Monitoring Arrangement

21.1 The Data Controller's Representative, together with the Data Protection Officer are responsible for monitoring and reviewing this policy.

21.2 The Data Controller's Representative, together with the Data Protection Officer check that the Academy complies with this policy by, among other things, reviewing records, policies and procedures annually.

21.3 This policy will be reviewed and updated as and when necessary, in relation to any amendments to Data Protection legislation or guidance, or any internal concerns resulting from policy violations, data breached, or on an annual basis.

21.4 At every review, the policy will be shared with the Governing Board.

22 Data Protection Officer (DPO) Contact Details

Data Protection Officer: Dee Whitmore. Email: dposervice@schoolspeople.co.uk
Telephone: 01773 851078
Postal Address: 44 Tyndall Court, Peterborough, Cambridgeshire, PE2 6LR.

ANNEX 1 - DEFINITIONS

Term	Definition
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes students, our staff, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a 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
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	are those of our staff (including Governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data 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. Processing also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data
Staff	Includes, any individual employed by the Academy and those who volunteer in any capacity including Governors, Members, Parents.

ANNEX 2 - Data Protection Security Procedures

The list below is a summary of data protection security procedures. The highlighted terms are not defined in this policy.

1. **Entry controls.** Any person not wearing appropriate identification should be approached and taken to reception to sign in. Any such person who has not been stopped should be reported immediately to the Property Team or the Senior Leadership Team to intervene.

2. **Secure lockable desks and cupboards.** Desks and cupboards should be locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

3. **Methods of disposal.**
   a) Paper documents containing personal data should be shredded. Arrangements are made on annual basis for large quantities of document shredding.
   b) Digital storage devices should be physically destroyed when they are no longer required. Digitally shredded hard drives and IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets e.g. Disposed through a WEEE registered company.

4. **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they lock their PC or laptop when it is left unattended.

5. **Working away from the Academy premises – paper documents.** Hard copy documents should not be removed from Academy if they contain personal data. Documents containing personal data are not to be printed out at home.

6. **Working away from the Academy premises – electronic working.**

   a) **USB devices** are not prohibited**,** but only use encrypted USB drives/laptops to backup media and if you need to take data off-site.

   b) Ensure your **wireless network at home is secure and encrypted**. WPA and WPA2 require users to provide a security key to connect.

   c) Work containing confidential information accessed remotely via the Academy network should ideally be though a Academy provided device e.g. encrypted laptop. Alternatively, if a non- Academy device has to be used in exceptional circumstances, then any downloaded files containing personal data should be erased after use and deleted from the recycle bin/trash folder.

   d) Use **secure remote access software** for accessing Academy systems from another location.

   e) Ensure your **home anti-virus/malware software** is updated regularly, along with the computers' operating system software.

7. **Document printing.** Documents containing **personal data** must be collected immediately from printers which are not 'Follow Me' printers. Photocopying must always be removed from the printer/photocopier at the time of copying

8. Personal data which can be accessed via an **electronic device (including a mobile phone)** must be password controlled and not be left 'open' for another person to access.

9. **Staff passwords** are automatically changed periodically with suitable complexity.

10. Consider **"Cyber Security"** when opening email attachments, scan USB devices and do not install software on your laptop/PC unless it comes from a known, reputable source.

11. **Manage personal filing** (paper and electronic) to ensure that documents containing personal data are only retained for the agreed retention periods.

The above security procedures are a summary only and do not include any detailed I.T security procedures undertaken by the Academy which will remain confidential.

Annex 3 - Data Security Breach Incident Management

Background
Data security breaches are increasingly common occurrences whether these are caused through human error or via malicious intent. As technology trends change and the creation of data and information grows, there are more emerging ways by which data can be breached. The academy needs to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly, protect its information assets and minimise the impact to any data subjects as far as practically a possible.

Aim
The aim of this policy annex is to standardise the academy response to any reported data breach incident, and ensure that such breaches are appropriately logged and managed in accordance with best practice guidelines.

By adopting a standardised consistent approach to all reported incidents, the academy will ensure that:
- incidents are reported in a timely manner and can be properly investigated
- incidents are handled by appropriately authorised and skilled personnel
- appropriate levels of academy management and directors (if applicable) are involved in response management
- incidents are recorded and documented
- the impact of the incidents are understood and action is taken to prevent further damage
- evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny
- external bodies or data subjects are informed as required
- the incidents are dealt with in a timely manner and normal operations restored
- the incidents are reviewed to identify improvements in policies and procedures.

Definition
A data security breach is considered to be “any loss of, or unauthorised access to, academy data”. Examples of data security breaches may include:
- Loss or theft of hard copy data or electronic equipment on which data is stored
- Unauthorised access to confidential or highly confidential data
- Equipment failure
- Human error for example incorrectly addressed emails
- Unforeseen circumstances such as a fire or flood
- Hacking/Phishing attack
- ‘Blagging’ offences where information is obtained by deceit

Data security breaches include both confirmed and suspected incidents.

Scope
This applies to all academy information, regardless of format, and is applicable to all staff, students, visitors, contractors and data processors acting on behalf of the academy.

Responsibilities
Information users

All information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

Heads of Faculty/Department

Heads of Faculty or Departments are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.

Assistant Head (Wider Curriculum)

Will collate and investigate any confirmed and suspected data breaches and report them to the DPO. Maintain the data breach log and report data breaches to the Head Teacher and governors.

Data Protection Officer

The Data Protection Officer will be responsible for overseeing the management of the breach in accordance with the Data Breach Management Plan and advising the Head Teacher. Suitable delegation may be appropriate in some circumstances.

Head Teacher

The Head teacher will implement the Data Breach Management Plan, working with the Data Protection Officer and other individuals as necessary.

Data Classification

Data security breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore it is important that the academy is able to quickly identify the classification of the data and respond to all reported incidents in a timely and thorough manner.

All reported incidents will need to include the appropriate data classification in order for assessment of risk to be conducted. Data classification referred to in this policy means the following approved categories:

Public Data

Information intended for public use, or information which can be made public without any negative impact for the academy.

Internal Data:

Information regarding the day-to-day business and academic operations of the academy. Primarily for staff and student use, though some information may be useful to third parties who work with the academy.

Confidential Data:

Information of a more sensitive and or personal nature required for the business and academic operations of the academy, representing basic intellectual capital and knowledge. Access should be limited to only those people that need to know as part of their role within the academy.

Highly confidential Data:

Information that, if released, will cause significant damage to the individual or academy's business activities or reputation, or would lead to breach of the UK GDPR and the Data Protection Act 2018. Access to this information must be highly restricted.

Data Security Breach Reporting

Confirmed or suspected data security breaches should be reported promptly to the Data Protection Officer (DPOService@Schoolpeople.co.uk). The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved. Where possible section 1 of the incident report form should be completed as part of the reporting process by the person initially reporting the incident. See **Appendix 1.**

Once a data breach has been reported the DPO will assess the severity of any personal data breach based on the number of data subjects involved, the data involved and the risks to the rights and freedoms of the data subject as a result of that breach All data security breaches will be centrally logged by the Data Protection Officer or delegated person to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes. The Data Protection Officer will be responsible for reporting appropriate breaches to the Information Commissioners Office (ICO).

Data Breach Management Plan

The management response to any reported data security breach will involve the following four elements. See **Appendix 2** for the checklist.

A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

Each of these four elements will need to be conducted in accordance with the checklist for Data Security Breaches. An activity log recording the timeline of the incident management should also be completed. See **Appendix 3.**

Authority

Staff, students, contractors, consultants, visitors and guests who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.

Review

The Personnel, Student Care and Discipline committee of the governing body will monitor the effectiveness of this policy and carry out regular reviews of all reported breaches.

References

Information Commissioner:
https://ico.org.uk/media/1562/guidance_on_data_security_breach_management.pdf

APPENDIX 1

Data Security Breach Form

Reference Number

//******

To be completed in all instances of an actual or suspected Data Security Breach.

Please act promptly to report any data breaches. Complete section 1 & 2 of this form and email it to the Internal Data Protection Lead - AHarwood@bishopstopford.com

Section 1: Notification of Data Security Breach *To be completed by the staff member reporting the incident.*	
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting the incident:	
Contact details of person reporting incident (email address, telephone number):	Email: Phone:
Brief description of the incident or details of the information lost:	
The number of Data Subjects affected if known:	
Details of the IT systems, equipment, devices, records involved.	
Details of hard copy data involved	
Brief description of any containment action taken at the time of discovery (Email recall, computer shut down, etc)	

Section 2: The nature of the data involved? **Please provide details of any types of information that fall into any of the following categories:**	
HIGH RISK personal data Special categories personal data (as defined in the Data Protection Legislation) relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions c) religious or philosophical beliefs; d) trade union membership; e) biometrics (where used for ID purposes) f) health/disability g) sex life or sexual orientation	
Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas, and other identity documents	
Personal information relating to children and vulnerable adults	
Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to persons if disclosed	
Information about individual cases of investigations, discipline or sensitive negotiations which could adversely affect individuals.	
Security information that would compromise the safety of individuals if disclosed.	

For use by the Data Protection Officer			
Received by:	Dee Whitmore	Date:	
Forwarded by			
Lead Investigating Officer appointed	Yes	Dee Whitmore - DPO	Email: DPOService@schoolpeople.co.uk Telephone: 01773 851078
Section 2: Assessment of Severity *To be completed by the Lead Investigation Officer in consultation with the Head of the area affected by the breach and if appropriate IT where applicable*			
Details of Information loss (defined as stolen or destroyed and not recoverable)			
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?			
Is the information unique? Will its loss have adverse operational, , financial legal, liability or reputational consequences for the organisation or third parties?			
How many data subjects are affected?			
Is the data bound by any contractual security arrangements?			
Data Protection Officer and/or Lead Investigation Officer to consider whether it should be escalated to the Governing Body			
Referral decision taken by:	Dee Whitmore. DPO		YES/NO
Section 3: Action Taken ***To be completed by Data Protection Officer and/or Lead Investigation Officer***			
Incident number		Completed by	
Was the incident reported to the Police?	YES/NO	Date reported	N/A
Follow up action required/recommended:			

For use of Data Protection Officer and/or Lead Officer:			
Notification to ICO	YES/NO	Date Reported	N/A
Details of Notification:-			
Notification to Data Subjects	YES/NO	Date Reported	N/A
Details of Notification			
Notification to other stakeholders	YES/NO	Date Reported	N/A
Details of Notification			
Notification to other stakeholders	YES/NO	Date Reported	N/A
Details of Notification			

Evaluation & Response	Date Reported completed	

APPENDIX 2

Data Breach Checklists

A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

Step	Action	Notes
A	**Containment and Recovery:**	**To contain any breach, to limit further damage as far as possible and to seek to recover any lost data.**
1	Data Protection Officer and Head Teacher to ascertain the severity of the breach and determine if any personal data is involved.	**See Appendix 2**
2	Data Protection Officer and Head Teacher to identify Lead Responsible Officer for investigating breach and forward a copy of the data breach report	To oversee full investigation and produce report. Ensure lead has appropriate resources including sufficient time and authority. If personal data has been breached also contact Br-Data-Protection. In the event that the breach is severe, the academy Incident Management Team will be contacted to lead the initial response.
3	Identify the cause of the breach and whether the breach has been contained? Ensure that any possibility of further data loss is removed or mitigated as far as possible	Establish what steps can or need to be taken to contain the breach from further data loss. Contact all relevant departments who may be able to assist in this process. This may involve actions such as taking systems offline or restricting access to systems to a very small number of staff until more is known about the incident.
5	Determine whether anything can be done to recover any losses and limit any damage that may be caused	E.g. physical recovery of data/equipment, or where data corrupted, through use of back-ups.
5	Where appropriate, the Lead Responsible Officer or nominee to inform the police.	E.g. stolen property, fraudulent activity, offence under Computer Misuse Act.
5	Ensure all key actions and decisions are logged and recorded on the timeline.	

B	Assessment of Risks	To identify and assess the ongoing risks that may be associated with the breach.
8	What type and volume of data is involved?	Data Classification/volume of individual data etc.
9	How sensitive is the data?	Sensitive personal data? By virtue of definition within Data Protection Act (e.g. health record) or sensitive because of what might happen if misused (banking details).
10	What has happened to the data?	E.g. if data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.
11	If the data was lost/stolen, were there any protections in place to prevent access/misuse?	E.g. encryption of data/device.
12	If the data was damaged/corrupted /lost, were there protections in place to mitigate the impact of the loss?	E.g., back up tapes/copies.
13	How many individuals' personal data are affected by breach?	
14	Who are the individuals whose data has been compromised?	Students, applicants, staff, customers, clients or suppliers?
15	What could the data tell a third party about the individual? Could it be misused?	Consider this regardless of what has happened to the data. Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
16	Is there actual/potential harm that could come to any individuals?	e.g. are there risks to: • physical safety; • emotional wellbeing; • reputation; • finances; • identify (theft/fraud from release of non-public identifiers); • or a combination of these and other private aspects of their life?
17	Are there wider consequences to consider?	E.g., a risk to public health or loss of public confidence in an important service we provide?

18	Are there others who might advise on risks/courses of action?	e.g. If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

C	**Consideration of Further Notification**	**Notification is to enable individuals who may have been affected to take steps to protect themselves or allow the regulatory bodies to perform their functions.**
19	Are there any legal, contractual or regulatory requirements to notify?	e.g.: terms of funding; contractual obligations
20	Can notification help the academy a meet its security obligations under the seventh data protection principle?	E.g., prevent any unauthorised access, use or damage to the information or loss of it.
21	Can notification help the individual?	Could individuals act on the information provided to mitigate risks (e.g. by changing a password or monitoring their account)?
22	If a large number of people are affected, or there are very serious consequences, inform the Information Commissioner's Office (through the Director of Information).	Contact and liaise with the Director of Legal Services or the Governance and Information Compliance Team.
23	Consider the dangers of 'over notifying'.	Not every incident will warrant notification "and notifying a whole 2 million strong customer base of an issue affecting only 2,000 customers may well cause disproportionate enquiries and work".
24	Consider whom to notify, what you will tell them and how you will communicate the message.	• There are a number of different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation. • Include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach. • When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what the institution is willing to do to help them. • Provide a way in which they can contact us for further information or to ask questions about what has occurred (e.g. a contact name, helpline number or a web page).

25	Consult the ICO guidance on when and how to notify it about breaches.	Where there is little risk that individuals would suffer significant detriment, there is no need to report. There should be a presumption to report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. Cases must be considered on their own merits and there is no precise rule as to what constitutes a large volume of personal data. Guidance available from http://www.ico.gov.uk/for_organisations/data_protection / the_guide/principle_7.aspx
26	Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals.	E.g. police, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies.

D	**Evaluation and Response**	**To evaluate the effectiveness of the academy's response to the breach.**
27	Establish where any present or future risks lie.	
28	Consider the data and contexts involved.	E.g. what data is held, its extent, sensitivity, where and how it is stored, how long it is kept.
29	Consider and identify any weak points in existing security measures and procedures.	E.g. in relation to methods of storage and/or transmission, use of storage devices, levels of access, systems/network protections.
30	Consider and identify any weak points in levels of security awareness/training.	Fill any gaps through training or tailored advice.
31	Report on findings and implement recommendations.	Report to Information Management and Security Board.

APPENDIX 3

Headings of Data Breach Log

No.	Your ref.	Details of breach						Consequences of breach
		Date of breach	No. people affected	Nature of breach (choose most relevant)	Description of breach	How you became aware of breach	Description of data	

Measures taken/to be taken				
All individuals informed?	Remedial action	Other Regulators informed	When did you first notify the ICO of the breach?	F&GP Governors advised