Diocese of Norwich
St Benet's
Multi Academy Trust

[Academy Name]

Data Protection, Subject Access, Information Security and Freedom of Information Publication Scheme Policy and Procedure

Policy Type:	**Trust Core Policy**
Approved By:	**Trust Board (Finance, Audit and Resources Committee)**
Approval Date:	**5 July 2021**
Date Adopted by LGB:	**dd/mm/yyyy**
Review Date:	**July 2024**
Person Responsible:	**Trust Data Protection Officer**

Summary of Changes

The model policy has been revised to reflect these changes to the statutory guidance as outlined below.

Page Ref.	Section	Amendment	Date of Change
	Throughout the document	Policy updated following Brexit and the adopting of the GDPR into UK law as the UK GDPR	April 2021
4	1.1	Updated to include the UK GDPR legislation Jan 2021 and statutory guidance including new guidance from the ICO	April 2021
4	4	Updated to include applicable data that falls under the UK GDPR	April 2021
7	5	Updated and section added to include new guidance for the role of the DPO and accountability	April 2021
7	6-7	Updated in line with guidance from the ICO and in line with UK GDPR requirements	April 2021
9	8	New section added to include reaffirmation regarding historical consent under EU GDPR	April 2021
10-17	9- 19	Renumbered in line with new sections added	April 2021
11	9.5.2	Updated the requirements around passwords	April 2021
18	Appendices	Appendix 2 updated to include online reporting Appendix 3 Privacy Notice for Parents and Guardians added Appendix 4 Subject Access Request template added	April 2021

Roles and Accountabilities

The Diocese of Norwich St Benet's Multi Academy Trust is accountable for all policies across its Academies. All policies, whether relating to an individual academy or the whole Trust, will be written and implemented in line with our ethos and values as articulated in our prospectus. We are committed to the provision of high quality education in the context of the Christian values of responsibility, respect and dignity where individuals are valued, aspirations are high, hope is nurtured and talents released.

A Scheme of Delegation for each academy sets out the responsibilities of the Local Governing Body and Principal / Head Teacher. The Principal / Head Teacher of each academy are responsible for the implementation of all policies of the Academy Trust.

All employees of the Trust are subject to the Trust's policies.

Contents

1. Purpose and legal framework

1.1. The purpose of this policy and procedure is to ensure compliance of the Diocese of Norwich St Benet's Multi Academy Trust ("the Trust") with all its obligations and with due regard to all relevant legislation and statutory guidance. These include, but are not limited to, the following:

- The UK General Data Protection Regulation (UK GDPR)
- Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- School Standards and Framework Act 1998
- Data Protection Act 2018

This policy also has regard to the following guidance.

- ICO (2021) "Guide to the UK General Data Protection Regulation (UK GDPR)
- DfE (2018) "Data protection: a toolkit for schools"

2. Data Controller and responding

2.1. The Trust is the Data Controller as defined in the United Kingdom General Data Protection Regulations Jan 2021 (UK GDPR).

2.1.1 The individual academy is the Data Processor as defined in the UK GDPR.

2.2. All **Freedom of Information (FOI)** requests will be dealt with by the Trust and academies should refer any such requests to the Chief Executive Officer.

2.3. Any FOI request from an individual for their own personally identifiable data is treated under the GDPR as a Subject Access Request (SAR) and can be dealt with by the individual academy. Otherwise an FOI that is:

a. complex; and/ or
b. potentially contentious; and/ or
c. has a reputational risk; and or
d. has a legal risk

should be referred to the Chief Executive Officer.

2.4. Day-to-day personally identifiable information / data requests should be dealt with by the academies Data Processor.

2.5. **If in doubt, refer any information request to the Trust Data Protection Officer.**

3. Notification with the UK's Supervisory Authority – the Information Commissioner's Office (ICO)

3.1. The Trust has notified the ICO via the appropriate template.

3.2. The Trust will renew the registration as required. In addition, if the Trust introduces any new purposes for processing personal information then it will notify the ICO by e-mail at notification@ico.gsi.gov.uk, requesting that the new purpose be included in the registration.

4. Applicable data and core rights of data subjects

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

4.2 ‘Sensitive personal data’ is referred to in the UK GDPR as ‘special categories of personal data’, and is defined as:

- Genetic data.
- Biometric data.
- Data concerning health.
- Data concerning a person’s sex life.
- Data concerning a person’s sexual orientation.
- Personal data which reveals:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Principles.

4.3 Under the requirements outlined in the UK GDPR, personal data will be:

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

  The UK GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with” the above principles. It also requires that data is processed responsibly by the Data Controller and Data Processor (defined in Section 2) under the accountability principle. Academies and central team will work together to ensure that there is a robust system in place to handle PII and document decisions taken about the processing activity.

4.4 The eight core rights of data subjects are summarized as follows:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

5. Accountability and Data Protection Officer (DPO)

5.1 The Trust is committed to being clear and transparent about what type of personal information we hold and how it is used. The Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR, and will provide comprehensive, clear and transparent privacy policies (see Appendix 3)

5.2 Additional internal records of the Trusts processing activities will be maintained and kept up to date held on site by individual academies. Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

5.3 The Trust will also document other aspects of compliance with the UK GDPR and Data Protection Act where this is deemed appropriate in certain circumstances by the DPO, including the following:

- Information required for privacy notices, e.g. the lawful basis for the processing
- Records of consent
- Controller-processor contracts
- The location of personal data
- Data Protection Impact Assessment (DPIA) reports
- Records of personal data breaches

5.4 The Trust and individual academies will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Minimising the processing of personal data.
- Pseudonymising personal data as soon as possible.
- Ensuring transparency in respect of the functions and processing of personal data.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

Data Protection Impact Assessments (DPIAs) will be used to identify and reduce data protection risks, where appropriate

5.5 A DPO will be appointed by the Trust in order to:

- Inform and advise the Trust and its employees about their obligations to comply with the UK GDPR and other data protection laws.
- Monitor the Trust's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on DPIAs, conducting internal audits, and providing the required training to staff members.
- Cooperate with the ICO and act as the first point of contact for the ICO and for individuals whose data is being processed.

5.6 The DPO is responsible for:

- Coordinating a proactive and preventative approach to data protection.
- Calculating and evaluating the risks associated with the Trust's data processing.
- Having regard to the nature, scope, context, and purposes of all data processing.
- Prioritising and focussing on more risky activities, e.g. where special category data is being processed.
- Promoting a culture of privacy awareness throughout the Trust and academy community.

The individual appointed as DPO will have professional experience and be highly knowledgeable about data protection law, particularly that in relation to academies. An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

The DPO will operate independently and will not be dismissed or penalised for performing their duties. Sufficient resources and appropriate access will be provided to the DPO to enable them to meet their UK GDPR obligations.

5.7 The DPO will report to the highest level of management at the Trust, which is the Trust Board. Staff will ensure that they involve the DPO in all data protection matters closely and in a timely manner.

6. Data Collection

6.1. The Trust is committed to being clear and transparent about what type of personal information we hold and how it is used. The Trust and academies will maintain internal records of processing activities. The Trust and individual academy will publish 'Privacy Notice for Pupils/Students and their Parents and Guardians' (Appendix 3) on both academy and Trust websites.

6.2. **Why do we collect information?**

6.2.1. The Trust collects information about our pupils and holds this personal data so that we can:

a. Support each pupil's learning;
b. Monitor and report on each pupil's progress;
c. Provide appropriate pastoral care and other support to each of our pupils; and
d. Assess how well each pupil is doing and report on that to the parents.

6.3. **What type of information do we collect?**

6.3.1. The information will include: personal data such as name and date of birth as well as contact details; educational performance assessments; attendance information; and, pastoral information. It will also include sensitive personal data such as: ethnicity; special educational needs; biometric data (fingerprint recognition – High School catering), behavioural incidents; and, medical information that will help us to support each pupil's education and wider welfare needs at the Trust. This information is collected directly from the parent/guardian or indirectly from the local authority or feeder school for example.

6.3.2. We will also hold personal contact information about parents and carers so that we can get hold of you routinely or in an emergency.

6.3.3. Where CCTV is used by the Trust this will is for security and the prevention and detection of crime.

6.3.4. Pupil photographs may be included as part of their personal data and this will be treated with the same level of confidentiality as all other personal data (see sections 13.2. and 15.1.).

6.4. **Do we share this information with anyone else?**

6.4.1. We do not share any of this data with any other organisation without your permission except where the law or governmental returns require it. We are required to provide pupil data to central government through the Department for Education (DfE) (www.education.gov.uk) and the Education Funding Agency (EFA) (www.education.gov.uk/efa). Where it is necessary to protect a child, the Trust will share data with agencies such as the Local Authority Children's Social Services and/or the Police.

6.5. **Can we see the personal data that you hold about our child?**

6.5.1. All pupils have a right to have a copy of all personal information held about them, with the exception of those identified in 6.5.3. A request for a copy of the personal information can be made by a parent or guardian in writing, but it should be remembered that the personal information belongs to the child (regardless of age) albeit the request may come from a parent or guardian. If we are confident that the child can understand their rights then we will respond to the child rather than a parent or guardian, taking into account that if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. Any

fees allowable under the GDPR (referenced in this document) may be waived in the case of a request from a child. When considering borderline cases of whether to release the information to the child we will take into account, among other things:

a. the age of the child, if aged 13 or over informed consent must be given by the young person, unless they have special needs which impact on their ability to make decisions like this:
b. the child's level of maturity and their ability to make decisions like this;
c. the nature of the personal data;
d. any court orders relating to parental access or responsibility that may apply;
e. any duty of confidence owed to the child or young person;
f. any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
g. any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
h. any views the child or young person has on whether their parents should have access to information about them.

6.5.2. Copies of examination scripts are not available for request.

6.5.3. Information would be withheld if there was a child protection risk, specifically:

a. The information might cause serious harm to the physical or mental health of the pupil or another individual;
b. Where disclosure would reveal a child is at risk of abuse;
c. Information contained in adoption or parental order records; and
d. Information given to a court in proceedings under the Magistrate's Courts (Children and Young Persons) Rules 1992.

6.5.4. To protect each child's right of confidentiality under law the Trust reserves the right to check the identity of a person making a request for information on a child's behalf. Once any identity check has been completed and any fee due paid, the information will be collected and provided within one calendar month.

6.6. **Can we see our child's educational record?**

6.6.1. All parents can request a copy of their child's educational record (noting Section 6.5). A request must be made in writing to the Trust. The Educational Record includes curriculum, assessment, pastoral and behavioural information that is stored by the Trust. Only information that has come from a teacher or employee of the Trust or an educational professional contracted by the Trust can be considered to form part of the educational record.

6.6.2. If you want a printed copy of the educational record the Trust will respond to the request within one calendar month.

7.Lawful Processing

7.1 The legal basis for processing data will be identified and documented prior to data being processed. Under the UK GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained
- Processing is necessary for a contract held with the individual, or because they have asked the school to take specific steps before entering into a contract
- Processing is necessary for compliance with a legal obligation (not including contractual obligations)
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for protecting vital interests of a data subject or another person, i.e. to protect someone's life

- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject – this condition is not available to processing undertaken by the school in the performance of its tasks

7.2 The Trust will only process personal data without consent where any of the above purposes cannot reasonably be achieved by other, less intrusive means or by processing less data.

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

- Explicit consent of the data subject
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- Processing relates to personal data manifestly made public by the data subject
- Processing is necessary for:

- Carrying out obligations under employment, social security or social protection law, or a collective agreement
- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- Reasons of substantial public interest with a basis in law which is proportionate to the aim pursued and which contains appropriate safeguards
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services with a basis in law
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with a basis in law

Where the Trust relies on:

- 'Performance of contract' to process a child's data, the academy considers the child's competence to understand what they are agreeing to, and to enter into a contract.
- 'Legitimate interests' to process a child's data, the academy takes responsibility for identifying the risks and consequences of the processing, and puts age-appropriate safeguards in place.
- Consent to process a child's data, the academy ensures that the requirements outlined in section 6 are met, and the academy does not exploit any imbalance of power in the relationship between the school and the child.

8.Consent

Consent must be a positive indication expressly confirmed in words. It cannot be inferred from silence, inactivity, a positive action without words or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Consent can be withdrawn by the individual at any time.

8.1 Where consent is given, a record will be kept documenting how and when consent was given, and what the data subject was told.

The Trust ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

8.2 Where the academy opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined above, the academy obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children. In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the school on a case-by-case basis, taking into account the requirements outlined above.

9. Information Security

9.1. Objective

9.1.1 The information security objective is to ensure that the Trust's information is protected against identified risks so that it may continue to deliver its services and obligations to the community. It seeks to ensure that any security incidents have a minimal effect on its business and academic operations.

9.2. Responsibilities

9.2.1. The Headteacher/Principal of the local academy has direct responsibility for maintaining the enforcing of this policy/procedure and for ensuring that the staff of the local academy adheres to it.

9.3. General Security

9.3.1. It is important that unauthorised people are not permitted access to Trust information and that we protect against theft of both equipment and information. This means that we must pay attention to protecting our buildings against unauthorised access. Staff must:

a. Not reveal pin numbers or building entry codes to people that you do not know or who cannot prove themselves to be employees;
b. Beware of people tailgating you into the building or through a security door;
c. If you don't know who someone is and they are not wearing some form of identification, ask them why they are in the building;
d. Not position screens on reception desks where members of the public could see them;
e. Lock secure areas when you are not in the office;
f. Not let anyone remove equipment or records unless you are certain who they are;
g. Ensure visitors and contractors in Trust buildings always sign in a visitor's book.

9.4. Security of Paper Records

8.4.1. Paper documents should always be filed with care in the correct files and placed in the correct place in the storage facility.

9.4.2. Records that contain personal data, particularly if the information is sensitive should be locked away when not in use and should not be left open or on desks overnight or when you are not in the office. Additionally, staff must:

a. Always keep track of files and who has them;
b. Not leave files out where others may find them;
c. Not, where a file contains confidential or sensitive information, give it to someone else to look after.

9.5. Security of Electronic Data

9.5.1. Most of our data and information is collected, processed, stored, analysed and reported electronically. It is essential that our systems, hardware, software and data files are kept secure from damage and unauthorised access. Staff must:

a. Prevent access to unauthorised people and to those who don't know how to use an item of software properly as it could result in loss of information and a breach of data leading to a subsequent fine for both academy and Trust;
b. Keep suppliers CDs/USB storage devices containing software safe and locked away and always label them so you do not lose them in case they need to be re-loaded;

c. Ensure that when we buy a license for software, it usually only covers a certain number of machines. Note: Make sure that you do not exceed this number as you will be breaking the terms of the contract.

9.5.2 Passwords are a critical element of electronic information security. All staff must manage their passwords in a responsible fashion and should not:

a. Write it down and keep it in an easily accessible place;
b. Give anyone your password;

All staff must ensure that:

c. The password should be at least 8 characters including upper and lower case;
d. The essential rules are that your password is something that you can remember but not anything obvious or predictable(e.g. “password”) or anything that people could guess easily (e.g. your name);
e. The password Include numbers as well as letters in the password;
f. They take care that no-one can see you type in your password;
g. They change the password regularly and use multi factor authentication to further strengthen security as part of the security factor offered by their ICT provider. Also you must change the password if you think that someone may know what it is.

9.5.3. You can be held responsible for any malicious acts by anyone to whom you have given your password.

9.5.4. Many database systems, particularly those containing personal data should only allow a level of access appropriate to each staff member. The level may change over time.

9.6. Use of E-Mail and Internet

9.6.1. The use of the Trust’s e-mail system and wider Internet use is for the professional work of the Trust. Reasonable personal use of the system in a member of staff’s own time is permitted but professional standards of conduct and compliance with the Trust’s wider policies are a requirement whenever the e-mail or Internet system is being used. The Trust uses a filtered and monitored broadband service to protect our pupils. Deliberate attempts to access websites that contain unlawful, pornographic, offensive or gambling content are strictly prohibited. Staff discovering such sites on the system must report this to their line manager immediately. The Headteacher/Principal will ensure that the sites are reported to the broadband provider for filtering.

9.6.2. To avoid a computer virus arriving over the Internet, do not open any flashing boxes or visit personal websites.

9.6.3. Filter and save important e-mails straight away.

9.6.4. Unimportant e-mails should be deleted straight away for example spam or unwanted subscription emails.

9.6.5. Do not send information by e-mail which breaches the General Data Protection Regulations. Check before sending that if the email contains personally identifiable information that the information is being processed lawfully, complies with the Privacy Notice (See Appendix 3) and if in doubt contact the Trust Data Protection Officer. Do not write anything in an e-mail which could be considered inaccurate or offensive, and cannot be substantiated.

9.7. Electronic Hardware

9.7.1. All hardware over the minimum threshold (see Finance Policy) held within Trust should be included on the asset register;

9.7.2. When an item is replaced the register should be updated with the new equipment.

9.7.3. Do not let anyone remove equipment unless you are sure that they are authorised to do so.

9.7.4. In non-secure areas, consider using clamps or other security devices to secure laptops and other portable equipment to desktops.

9.8. Homeworking Guidance

9.8.1. If staff work outside of the Trust or at home, all of the principles contained in this policy/procedure still apply. However, working outside of the Trust presents increased risks for securing information. The following additional requirements apply:

a. Do not access confidential information when you are in a public place, such as a train, where you may be overlooked;
b. Do not have conversations about personal or confidential information on your mobile when in a public place. Ensure that, if urgent, you have your conversation in a separate room or away from other people;

9.8.2. If you use a laptop or tablet or smart phone:

a. Ensure that it is locked and password protected to prevent unauthorised access;
b. Make sure that you don't leave your device anywhere it could be stolen. Keep it with you at all times and secure it when you are in the Trust. Any loss of data must be immediately reported to the Trust Data Protection Officer as confirmed breaches of data have to be reported to the ICO within **72 hours** and this timeframe is not 3 working days but will include the weekend.
c. Data held must be encrypted (either the laptop or external storage – see 9.8.3)

9.8.3. Any portable device or memory stick that contains personal data must be encrypted. Personal data may not be taken off the Trust's site or put onto a portable device without the express permission of the Headteacher/Principal. Taking personal data off-site on a device or media that is not encrypted could be a disciplinary matter

9.8.4. When working on confidential documents at home do not leave them lying around where others may see them; dispose of documents using a shredder.

9.8.5. If you are using your own computer, ensure that others cannot access documents. It is **recommended** that you access the documents on an encrypted device (rather than transferring them onto your computer). If you do need to transfer documents onto your computer, when you have completed working on them transfer them back to the Trust's system or encrypted storage device and delete them from your computer (including emptying the 'recycle bin'). It is forbidden to use a computer owned by you, other than for short periods specified above, to hold personal data about pupils or staff of the Trust.

9.9. Audit of Data Access

9.9.1. Where possible our software specifications will include the function to audit access to confidential data and attribute access, including breaches of security, to specific users.

9.10. Data Backup

9.10.1. The Trust has reviewed its procedures for ensuring that all critical and personal data is backed-up to secure online (off physical site) storage.

9.10.2. Data backup should routinely be managed on a rolling daily process to secure off-site areas.

10. Disposal of Information

10.1. Paper records should be disposed of with care. If papers contain confidential or sensitive information shred them before disposing of them. Particular care must be taken when selecting papers to be placed in a recycling bin.

10.2. Computers and hardware to be disposed of must be completely 'wiped'/'cleaned' before disposal. It is not enough just to delete all the files.

10.3. It cannot be assumed that simply deleting a file will prevent it being recovered from electronic media. Electronic memory containing personal information or sensitive personal information must be electronically scrubbed or physically destroyed.

10.4. Where a third-party contractor holds personal information on behalf of the Trust (e.g. payroll provider), the Trust will agree and document an appropriate allocation of information security roles and responsibilities to ensure the contractor fulfils their obligations as Data Processor under the UK GDPR.

11. Subject Access Requests

11.1. Requests from parents or pupils for access to personal data or educational records will be dealt with as described in Section 6 and using the Trust SAR template (Appendix 4)

11.2. Trust staff may have access to their personal data within one calendar month of a request and at no charge.

11.3. The Trust will maintain a documented record of all requests for personal information with details of who dealt with the request, what information was provided and when, and any outcomes. The record will be used if there is a subsequent complaint in relation to the request.

12. Sharing Personal Information

12.1. The Trust only shares personal information with other organisations where there is a legal requirement to do so or the organisation has been contracted by the Trust to carry out a function of the Trust.

12.2. The Trust is required, for example, to share information with the Department for Education and the Education Funding Agency. Under certain circumstances, such as child protection, we may also be required to share information with Children's Social Services or the Police.

12.3. Because our pupils are of school age, their own right to access their own personal information held by the Trust will be typically, but not always, exercised through their parents or guardians (see Section 6) unless they have reached the age of 13 years.

12.4. The Headteacher/Principal will be responsible for authorising the sharing of data with another organisation. The principle in authorising the sharing of data will take account of:

12.4.1. Whether it is lawful to share it (following guidance from the Trust Data Protection Officer);

12.4.2. Whether there is adequate security in place to protect the information while it is being transferred and then held by the other organisation;

12.4.3. Include in the Privacy Notice a simple explanation of who the information is being shared with and why.

12.5. Considerations regarding the method of transferring data should include:

12.5.1. If personal data is sent by e-mail then security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending the message. The data may also need to be password protected and the password sent separately. You should also check that it is going to the correct e-mail address.

12.5.2. Circular e-mails sent to parents should be sent bcc (blind carbon copy) so that the e-mail addresses are not disclosed to everyone.

12.5.3. Similar considerations apply to the use of fax machines. Ensure that the recipient will be present to collect a fax when it is sent and that it will not be left unattended on their equipment.

12.5.4. If confidential personal data is provided by paper copy it is equally important to ensure that it reaches the intended recipient.

13 Personal Data Breach

13.1 A personal data breach refers to a protection breach that results in the loss, destruction, alteration, unauthorised disclosure, or access to, personal data. In many cases reporting of a data breach is mandatory.

13.2 If a breach of personal data occurs or is suspected to have occurred, academies must report this immediately via the Trust website – staff secure area. This will automatically be routed to the DPO for review. (See Appendix 1 for Internal Breach Reporting Procedures) A risk assessment template (see

Appendix 2) will be completed by the Data Protection Officer and returned to the academy with further advice and guidance and/or confirmation of reporting to the Information Commissioners Officer by the individual academy/Trust Data Protection Officer.
NB The Trust has up to **72 hours** from the time it has established a breach has occurred, to report the breach to the Information Commissioners Office (SA)

14. Websites

14.1. The Trust website will be used to provide important information for parents and pupils including our Privacy Notice and our Freedom of Information publication scheme.

14.2. Where personal information, including images, are placed on the website the following principles apply:

14.2.1. We will not disclose personal information (including photos) on a website without the consent of the pupil, parent, and member of staff or Governor as appropriate (see sections 8 and 16.1.);

14.2.2. Comply with regulations regarding cookies and consent for their use;

14.2.3. Our website design specifications will take account of the principles of data protection regulations.

15. CCTV

15.1. The Trust uses CCTV and this has been notified to the Information Commissioners Office along with the purpose of capturing images using CCTV. The Trust appreciates that images captured on CCTV constitute personal information under the GDPR.

16. Photographs

16.1. The academy will comply with the UK GDPR and request parents' / guardians' / staff permission before taking images of pupils or members of the Trust. Subsequently, **if permission has been granted**, the Trust may use photographic images of pupils in publicly available media such as websites, newsletters or the academy prospectus. Also see sections 8. and 14.2.

16.2. Images recorded by parents using their own personal equipment of their child in a school play or activity for their own family use are not covered by data protection legislation.

16.3. To respect everyone's privacy, and in some cases protection, images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images (see E-safety and ICT Acceptable Use Policy on our website).

16.4. All other uses by the Trust of photographic images are subject to current data protection regulations.

17. Processing by Others

17.1. The Trust remains responsible for the protection of data that is processed by another organisation on its behalf. As part of a contract of engagement other organisations that process data on behalf of the Trust will agree and document an appropriate allocation of information security roles and responsibilities to ensure the contractor fulfils their obligations as Data Processor under the GDPR.

18. Training

18.1. The Headteacher/Principal will ensure that all staff are adequately trained to understand their responsibilities in relation to this policy and procedures.

19. Freedom of Information Publication Scheme

19.1. In line with the Freedom of Information Act the Trust will provide its Approved Publication Scheme on its website. Valid written requests under the Freedom of Information Act will normally be responded to within 40 calendar days, although we will endeavour to respond quicker.

Information to be published	*How the information can be obtained*	*Cost*
Class 1 – Who we are and what we do		
Who's who in the school	School Prospectus / Website	Free
Who's who on the governing body and the basis of their appointment	School Prospectus / Website	Free
Scheme of Delegation	Request via Head Office	Free
Contact details for the Head teacher – telephone number and email address	School Prospectus / Website	Free
School prospectus	School Office / e-mail / Website	Free
Staffing structure	Website	Free
Class 2– What we spend and how we spend it		
(Financial information relating to projected and actual income and expenditure, procurement, contracts and financial audit)		
Annual accounts	Trust Website	Free
Value for Money statement	Trust Website	Free
Pay policy	Trust Website	Free
Governor / trustee allowances policy	Trust Website	Free
Finance policy	Trust Website	Free
Class 3 – What our priorities are and how we are doing		
(Strategies and plans, performance indicators, audits, inspections and reviews)		
The latest full Ofsted reports	Website	Free
Monitoring and evaluation of T&L	Website	Free
School profile Government supplied performance data	Website	Free
Class 4 – How we make decisions		
(Decision making processes and records of decisions) Current and previous three years as a minimum		
Admissions policy (not individual admission decisions)	Trust and Academy Website	Free
Agendas of meetings of the local governing body and (if held) its committees	Website	Free

Minutes of meetings (as above) – n.b. this will exclude information that is properly regarded as private to the meetings.	Website	Free

Class 5 – Our policies and procedures

(Current written protocols, policies and procedures for delivering our services and responsibilities). Current information only

School policies / procedures including:		
Charging and remissions policy	Trust Website	Free
Health and Safety	Trust Website	Free
Complaints	Trust Website	Free
Staff bullying & harassment	Trust Website	Free
Staff discipline, conduct and grievance	Trust Website	Free
Staff appraisal	Trust Website	Free
Lone working	Trust Website	Free
Recruitment & selection	Trust Website	Free
Medical / medicines for pupils	Trust Website	Free
Staff whistleblowing	Trust Website	Free
Capability	Trust Website	Free
Child protection & safeguarding	Trust Website	Free
Allegations of abuse against staff	Trust Website	Free
Anti-bullying (pupils)	Trust Website	Free
Home-school agreement	School Prospectus / Website	Free
Curriculum	School Prospectus / Website	Free
Sex education	School Prospectus / Website	Free
Staff leave of absence	Trust Website	Free
Special educational needs	Trust and Academy Website	Free
Accessibility plan	Trust Website	Free
Collective worship	Trust Website	Free
Religious education	Trust Website	Free
Pupil discipline / behaviour	School Prospectus / Website	Free
Sickness absence management	Trust Website	Free
Staff wellbeing	Trust Website	Free
E-safety and ICT acceptable use	Trust Website	Free
Data protection (including information security, freedom of information and subject access requests)	Trust Website	Free

Class 6 – Lists and Registers

Curriculum circulars and statutory instruments	Website/ Newsletters	Free
Any information the school is currently legally required to hold in publicly available registers (This will not ordinarily include the attendance register as publishing would normally breach data protection principles)	Hard copy	10p/sheet

Class 7 – The services we offer

(Information about the services we offer, including leaflets, guidance and newsletters produced for the public and businesses) Current information only

Extra-curricular activities	Prospectus / Website /	Free
Out of school clubs	Newsletters	Free
Leaflets books and newsletters	Prospectus / Website / Newsletters Website/ School Office	Free

Schedule of charges

This describes how the charges have been arrived at and should be published as part of the guide.

Type of charge	*Description*	*Basis of charge*
Disbursement cost	Photocopying/printing @ 10p per sheet (black and white)	Approx. cost
Postage	Royal Mail standard 2nd Class	Actual cost

Contact details

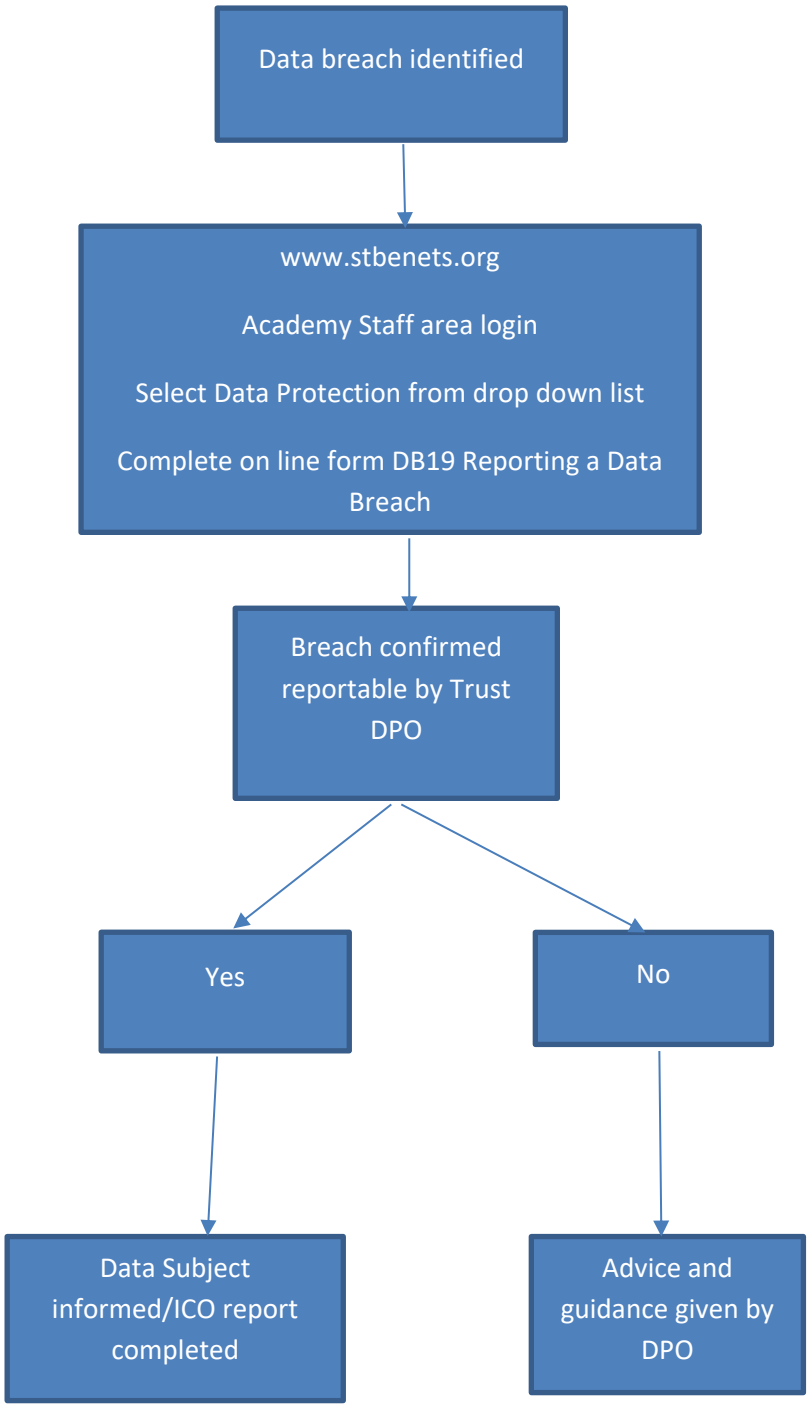
Chief Executive Officer
St Benet's MAT
Diocesan House
109 Dereham Road
Easton
Norwich
NR9 5ES

Tel: 01603 882327
www.sbenets.org

Data Protection Officer
Diocese of Norwich Education Services Company
Sharon Money
Diocesan House
109 Dereham Road
Easton
Norwich
NR9 5ES

Tel: 01603 882329
sharon.money@donesc.org

Appendix 1 Reporting an Internal Data Breach



Appendix 2
Risk assessment/confirmation of reportable breach completed by DPO

Recital 85 of the GDPR states that :
"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

Actions undertaken by [insert name of academy]

[insert actions taken in time/date order and by whom]

Risk assessment undertaken [insert date] by the Trust DPO

Using the following Risk Rating your case has been deemed to be Low/Medium/High [delete as applicable] and it is the recommendation of the DPO that in this case this breach is/is not reportable [delete as applicable] to the ICO

Rating	0	1	2	3	4	5	6
Reputation	No significant reflection on any individual or body Media interest very unlikely.	Damage to an individual's reputation. Possible media interest (e.g. prominent member of the Trust involved).	Damage to an Academy/ Trust reputation. Some local or national subject specific media interest that may not go public.	Damage to the Trust's reputation. Low key local or national media coverage.	Damage to The Trust/Church of England's reputation. Local media coverage.	Damage to the Trust/ Church of England/National media coverage.	Monetary penalty Imposed by ICO.
Clients potentially affected	Minor breach of confidentiality. Only a single individual affected.	Potentially serious breach. Less than five individuals affected, or risk assessed as low (e.g. files were encrypted).	Serious potential breach and risk assessed high (e.g. unencrypted sensitive/health records lost) Up to 20 individuals affected.	Serious breach of confidentiality e.g. up to 100 individuals affected and/or identifiable or particularly sensitive ie redundancies/restructuring.	Serious breach with either a particular sensitivity (e.g. sexual or mental health details, or up to 1000 individuals affected.	Serious breach with potential for ID theft or over 1000 individuals affected.	Restitution to injured parties. Other Liabilities. Additional security. Legal costs.
Communications	Maintain internal communications to staff members	Maintain internal communications to the staff members/MAT CEO GDPR Trustee/Bishops Press Officer.	Maintain internal communications to the staff members/ MAT CEO GDPR/Trustee/ Bishops Press Officer. Also inform the individuals affected as well as the ICO.	Maintain internal communications to the MAT CEO Trust Board Bishops Press Officer./ Also inform the individuals affected as well as the ICO.	Maintain internal communications to the MAT CEO Trust Board/Diocese Bishops Press Officer./ Also inform the individuals affected as well as the ICO.	Maintain internal communications to the MAT CEO Trust Board/Diocese Bishops Press Officer./. Also inform the individuals affected as well as the ICO.	Maintain internal communications to the MAT CEO Trust Board/Diocese Bishops Press Officer./. Also inform the individuals affected as well as the ICO.

Privacy Notice for Parents

How we use pupil and student information

Who is responsible for this information?

[insert name of academy] is the Data Controller for the use of personal data in this privacy notice.

The categories of pupil information that we process include:

- personal identifiers and contacts (such as name, unique pupil number, contact details and address)
- characteristics (such as ethnicity, language, and free school meal eligibility)
- safeguarding information (such as court orders and professional involvement)
- special educational needs (including the needs and ranking)
- medical and administration (such as doctors' information, child health, dental health, allergies, medication and dietary requirements)
- attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- assessment and attainment (such as key stage 1 and phonics results, post-16 courses enrolled for and any relevant results)
- behavioural information (such as exclusions and any relevant alternative provision put in place)

This list is not exhaustive, to access the current list of categories of information we process please see [insert link to website].

Why we collect and use pupil information:

The personal data collected is essential for the academy to fulfil their official functions and meet legal requirements.

We collect and use pupil information for the following purposes:

a) to support pupil learning
b) to monitor and report on pupil attainment progress
c) to provide appropriate pastoral care
d) to assess the quality of our services
e) to keep children safe (food allergies, or emergency contact details)
f) to meet the statutory duties placed upon us by the Department for Education

Under the General Data Protection Regulation UK (GDPR UK), the lawful bases we rely on for processing pupil information are:

- for the purposes of a), b), c) and d) in accordance with the legal basis of Public task: collecting the data is necessary to perform tasks that schools are required to perform as part of their statutory function
- for the purposes of e) in accordance with the legal basis of Vital interests: to keep children safe (food allergies, or medical conditions)
- for the purposes of f) in accordance with the legal basis of Legal obligation: data collected for DfE census information
- Section 537A of the Education Act 1996
- the Education Act 1996 s29(3)
- the Education (School Performance Information) (England) Regulations 2007
- regulations 5 and 8 School Information (England) Regulations 2008
- the Education (Pupil Registration) (England) (Amendment) Regulations 2013

In addition, concerning any special category data:

- in the case of ethnicity and fingerprint information: condition a: the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject

Collecting pupil information:

We obtain pupil information via registration forms at the start of each academic year. In addition, when a child joins us from another school, we are sent a secure file containing relevant information.

Pupil data is essential for the academy's' operational use. Whilst most of the pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with GDPR UK we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if you have a choice in this and we will tell you what you need to do if you do not want to share this information with us.

Storing pupil data:

We hold pupil data securely for the set amount of time shown in our data retention schedule. For more information regarding our data retention schedule and how we keep your data safe, please visit [insert link to website].

Who we share pupil information with:

We routinely share pupil information with:

- the school that the pupil attends after leaving us
- our local authority
- youth support services (pupils aged 13+)
- the Department for Education (DfE)
- Local Authorities

Why we routinely share pupil information:

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

Youth support services:

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

This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or guardian can object to any information in addition to their child's name, address and date of birth being passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once they reach the age of 16.

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

This enables them to provide services as follows:

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

A child / pupil once they reach the age of 16 can object to only their name, address and date of birth is passed to their local authority or provider of youth support services by informing us.

Data is securely transferred to the youth support service via a secure file transferring system and is stored within local authority software.

For more information about services for young people, please visit our local authority website: [insert link to relevant local authority website].

Department for Education:

We are required to share information about our pupils with the Department for Education (DfE) either directly or via our local authority for the purpose of data collections, under:

- Section 537A of the Education Act 1996
- the Education Act 1996 s29(3)
- the Education (School Performance Information) (England) Regulations 2007
- regulations 5 and 8 School Information (England) Regulations 2008
- the Education (Pupil Registration) (England) (Amendment) Regulations 2013

All data is transferred securely and held by the DfE under a combination of software and hardware controls, which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

Local Authorities:

We may be required to share information about our pupils with the local authority to ensure that they can conduct their statutory duties under

- the Schools Admission Code, including conducting Fair Access Panels

Requesting access to your personal data:

Under GDPR UK, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the academy office [insert contact details here] or the Trust Data Protection Officer, Sharon Money, by email at sharon.money@donesc.org or on 01603 882329.

Depending on the lawful basis above, you may also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance by contacting the Trust Data Protection Officer or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/.

Withdrawal of consent and the right to lodge a complaint:

Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting the academy office [insert contact details here] or the Trust Data Protection Officer, Sharon Money, by email at sharon.money@donesc.org or on 01603 882329.

Last updated:

We may need to update this privacy notice periodically, so we recommend that you revisit this information from time to time. This version was last updated on 17 March 2021.

Contact:

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

- The Trust Data Protection Officer, Sharon Money, by email at sharon.money@donesc.org or on 01603 882329
- Our local authority at [insert link to relevant local authority website]

How Government uses your data:

The pupil data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school
- informs 'short term' education policy monitoring (for example, school GCSE results or Pupil Progress measures)
- supports 'longer term' research and monitoring of educational policy (for example, how certain subject choices go on to affect education or earnings beyond school)

Data collection requirements:

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

The National Pupil Database (NPD):

Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD). The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department.

It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.
To find out more about the NPD, go to:
https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information

Sharing:

The law allows the DfE to share pupils' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

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

Organisations fighting or identifying crime may use their legal powers to contact the DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, the DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the DfE has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website:
https://www.gov.uk/government/publications/dfe-external-data-shares

How to find out what personal information DfE hold about you:

Under the terms of the Data Protection Act 2018, you are entitled to ask the DfE:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they are holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the DfE, you should make a 'subject access request'. Further information on how to do this can be found within the DfE's personal information charter that is published here: https://www.gov.uk/guidance/hmrc-subject-access-request.

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

Appendix 4 Subject Access Request Template

Date

Dear

Subject Access Request
I acknowledge your email/verbal request/letter on [insert date] for a Subject Access Request in regard to xxxx.

Please note that I have to/have confirmed the identify of yourself as the parent/guardian of the data subject and, once confirmed, the academy has one calendar month to respond to your request from [insert date].

Please also note that any personally identifiable information relating to a third party whose consent to disclosure of their personal information has not been given or information which may put a child at risk (under safeguarding legislation) will be redacted from any records given to you.

I require to you undertake the following:

1. Please contact the academy to confirm if you wish for the information to be supplied in hard copy or electronic format.

2. Confirm the Subject Access Request is for the following records and please confirm this to the academy:
· Obtain minutes from meeting xxxxxxx [insert what was requested]
· Minutes/record of incident xxxxxxxx

The academy can then contact you when the information is ready and you can make arrangements to collect and sign for the records/or to have them securely transferred electronically.

Yours sincerely

Headteacher/Principal/Head of School