Kessingland
Church of England
Primary Academy

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

Policy Type:	**Trust Core Policy**
Approved By:	**DNEAT Trust Board**
Approval Date:	**27/09/2019**
Date Adopted by LGB:	**10/10/2019**
Review Date:	**September 2022**
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
5	5	Amended to include the 8 core rights of data subject (audit requirement)	August 2019
5	4.3	Section added guidance on the nature of consent to be obtained (audit requirement)	August 2019
6	7.2	Including collection of personal data indirectly from a third party	August 2019
20	Appendices	Appendix 2 Identification of a reportable breach (audit requirement/DPO risk assessment)	August 2019

Contents

1. Purpose

1.1. The purpose of this policy and procedure is to ensure compliance of the Diocese of Norwich Education and Academies Trust ("the Trust") with all its obligations as set out in the Data Protection Regulations and Freedom of Information legislation.

2. Data Controller and responding

2.1. The Trust is the Data Controller as defined in the European Union General Data Protection Regulations May 2018 (GDPR).

2.1.1 The individual academy is the Data Processor as defined in the GDPR May 2018.

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. Definitions

4.1. Personally identifiable Information (PII) is any information relating to an identified natural person who can be identified, directly or indirectly. In particular in reference to an identifier such as emails, names of staff and pupils, dates of birth, addresses, national insurance numbers, IP addresses, school marks, medical information, exam results, SEN assessments and staff development reviews. PII only relates to living natural persons, not a corporate i.e. legal person.

Processing means collecting, using, transmitting, adapting or modifying, disclosing, retaining, or disposing of information. The EU GDPR data protection regulations apply to all information held electronically or in structured files that can identify, directly or indirectly to a living individual. The principles also extend to all information in education records.

4.2. Sensitive personal data is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, biometric data, physical or mental health, sexuality and criminal offences. There are greater legal restrictions on processing sensitive personal data than there are on personal data.

4.3 Consent should be given by a clear affirmative act… such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent.

5. Data Protection Regulations Principles and Rights

5.1. The seven principles of the General Data Protection Regulations are enshrined in this policy and in the Trust's commitment that personal data:

I. is processed lawfully and with fairness and transparency;

II. is collected for specified, legitimate and explicit purpose and must not be further processed in such a way which is incompatible with such purposes;

III. is relevant, adequate and limited to what is necessary in relation to the purposes for which that data is processed;

IV. is accurate and up to date and actions should be taken to avoid storing old or redundant data and to ensure that inaccurate personal data, with regard to the purposes for which they are processed, should be erased or rectified without delay.;

V. is kept in a form that permits the identification of Data Subjects for no longer than is necessary, for the purposes for which the personal data is 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, or statistical purposes e.g. pupil attainment and in accordance with the measures required by the GDPR

VI. is processed in accordance with the eight core rights of data subjects under the GDPR and processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical, or organisational methods;

VII. 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

VIII. is processed responsibly by the Data Controller and Data Processor (defined in Section 2) under the accountability principle and 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.

6. Fair Processing

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 following 'Privacy Notice for Pupil and their Parents and Guardians' will be published on the Trust's website.

7. Privacy Notice for Pupils and their Parents and Guardians

7.1. Why do we collect information?

7.1.1. 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.

7.2. What type of information do we collect?

7.2.1. 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.

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

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

7.2.4. 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 12.2. and 14.1.).

7.3. Do we share this information with anyone else?

7.3.1. 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.

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

7.4.1. All pupils have a right to have a copy of all personal information held about them, with the exception of those identified in 7.4.3. and 7.4.4. 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.

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

7.4.3. 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.

7.4.4. 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.

7.5. Can we see our child's educational record?

7.5.1. All parents can request a copy of their child's educational record (noting Section 7.). 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.

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

8. Information Security

8.1. Objective

8.1.1. 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.

8.2. Responsibilities

8.2.1. 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.

8.3. General Security

8.3.1. 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.

8.4. 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.

8.4.2. 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.

8.5. Security of Electronic Data

8.5.1. 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.

8.5.2. Passwords are a critical element of electronic information security. All staff must manage their passwords in a responsible fashion, including:

a. Don't write it down;
b. Don't give anyone your password;
c. Your password should be at least 8 characters;
d. The essential rules your password is something that you can remember but not anything obvious (e.g. "password") or anything that people could guess easily (e.g. your name);
e. Include numbers as well as letters in the password;
f. Take care that no-one can see you type in your password;
g. Change your password regularly and when prompted. Also change it if you think that someone may know what it is.

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

8.5.4. 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.

8.6. Use of E-Mail and Internet

8.6.1. 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.

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

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

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

8.6.5. 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 section 7) 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.

8.7. Electronic Hardware

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

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

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

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

8.8. Homeworking Guidance

8.8.1. 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;

8.8.2. 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 8.8.3)

8.8.3. 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

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

8.8.5. 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.

8.9. Audit of Data Access

8.9.1. 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.

8.10. Data Backup

8.10.1. The Trust is reviewing its procedures for ensuring that all critical and personal data is backed-up to secure online (off physical site) storage. Currently, accounts, payroll and pupil data is cloud based, and the Trust central server is backed-up off-site.

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

9. Disposal of Information

9.1. 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.

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

9.3. 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.

9.4. 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 GDPR.

10. Subject Access Requests

10.1. Requests from parents or pupils for access to personal data or educational records will be dealt with as described in the Privacy Notice for Pupils and their Parents and Guardians (see Section 7 above).

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

10.3. 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.

11. Sharing Personal Information

11.1. 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.

11.2. 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.

11.3. 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 7) unless they have reached the age of 13 years.

11.4. 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:

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

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

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

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

11.5.1. 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.

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

11.5.3. 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.

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

12 Personal Data Breach

12.1 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.

12.2 If a breach of personal data occurs or is suspected to have occurred, academies must contact the Trust Data Protection Officer immediately. (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)

13. Websites

13.1. 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.

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

13.2.1. 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 7.2.4. and 14.1.);

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

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

14. CCTV

14.1. 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.

15. Photographs

15.1. The academy will comply with the 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 7.2.4. and 13.2.

15.2. 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.

15.3. 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).

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

16. Processing by Others

16.1. 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.

17. Training

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

18. Freedom of Information Publication Scheme

18.1. 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 / Newsletters	Free
Out of school clubs	Prospectus / Website / Newsletters	Free
Leaflets books and 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
DNEAT
Diocesan House
109 Dereham Road
Easton
Norwich
NR9 5ES

Tel: 01603 882327
www.dneat.org

Data Protection Officer
DNEAT
Sharon Money
Diocesan House
109 Dereham Road
Easton
Norwich
NR9 5ES

Tel: 01603 882329
sharon.money@dneat.org

Appendix 1
Reporting Internal Data Breach
To be emailed to the Trust Data Protection Officer immediately a data breach is discovered
HIGHLY CONFIDENTIAL

FORM FOR REPORTING A SUSPECTED INFORMATION SECURITY INCIDENT		
YOUR NAME:		ACADEMY NAME/CENTRAL OFFICE
Today's Date:	Tel No:	E-MAIL ADDRESS:

…..

Date of Incident:	Time of Incident:
Who Was Notified:	Time of Notification:
Brief Description of Incident: (include website URLs, suspect name(s), impacted system(s), other relevant data...)	

	Y	N
Did you witness the incident yourself?	☐	☐
Did others witness the incident? (if yes, specify below)	☐	☐

To your knowledge was any of the following involved?

Telephone	☐	Theft	☐
Fax	☐	Fraud	☐
Photocopier	☐	Unauthorised Access	☐
Computer Hardware/Memory stick	☐	Customers	☐
E-mail	☐	Third Parties	☐
Internet download	☐	Copyright	☐
Virus	☐	Other (specify below)	☐

	Y	N
Was any individual Internal/External or Confidential information compromised?	☐	☐
Did you report this incident to: (Please circle all applicable Headteacher ICT – Other (Please Specify)	☐	☐

For DNEAT Office use only

Initiated By:	Date:	Confirmed breach Y/N:	Date:
Approved By (1):	Date:	Reported to the ICO:	Date:

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.