TRUST GDPR, DATA PROTECTION AND FOI POLICY

Version	2.1
Date	02/01/2018
Approved by Board of Directors	

Version	Date	Description	Revision author
1.0	02/01/2018	New Trust GDPR, Data Protection and FOI Policy created to replace the Trust Data Protection and FOI Policy to reflect the new General Data Protection Regulations from 25 May 2018.	FMW
2.0	Mar-18	Reviewed	GD
2.1	Sept - 18	Reviewed to reflect changes in final draft of legislation	AV

Contents

1. GDPR and Data Protection Introduction

Beckfoot Trust is required to keep and process certain information about its staff and students in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

This policy is in place to ensure the Trust Board and all Trust staff are aware of their responsibilities and it outlines how the Trust and Trust schools comply with the following core principles of the GDPR.

Organisational and technical methods for keeping data secure are imperative, therefore Beckfoot Trust have implemented a **Trust Privacy Compliance Framework** – see **Appendix 1**.

2. Legal framework

This policy has due regard to legislation, including, but not limited to the following:

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

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

This policy will be implemented in conjunction with the following Trust policies, procedures;

- Trust GDPR, Data Protection and Freedom of Information Policy
- Trust CCTV Policy (Localised School Version)
- Trust Online Safety, ICT and Social Media Policy (inc. Photography and Videos)
- Trust Child Protection and Safeguarding Policy
- Trust Records Management Policy
- Trust Data Protection Impact Assessments (DPIA) Procedure
- Trust Data Breach Management Procedure
- Trust Data Subject Access Request Procedure
- Trust Business Continuity Policy (and school local policies)

3. Controller and Processor

Beckfoot Trust and Trust schools are both a **"Controller"** and **"Processor"** of personal data. Beckfoot Trust are registered as a "Controller" with the Information Commissioner's Office.

- A "**Controller"** determines the purpose and means of processing personal data.
- A data "**Processor"** processes personal data on behalf of the data controller.

4. Applicable data

For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual e.g. Employee, Candidate, Student, Parent/Carer, Volunteer, Contractor, Freelancer, Board Member, and LSC Member. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria:-

- **Personal data** includes information such as name, address, DOB, NI Number; email address (personal and business), chronologically ordered data and pseudonymised data e.g. UPN numbers, Admission Numbers, Employee Numbers, key-coded data and online identifiers, e.g. IP addresses.
- **Sensitive personal data** is referred to in the GDPR as '**special categories of personal data**', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of racial or ethnic origin, political opinions, religious or philosophical beliefs, Trade Union membership, genetic data, biometric data, health, sex life and sexual orientation. In schools this could also be staff sickness absence, diversity monitoring, photos etc. **There are strict rules surrounding the processing of special categories of personal data.**

5. Principles

In accordance with the requirements outlined in the GDPR, personal data **must** be:-

- Processed lawfully
- For a specific purpose
- Kept to a minimum
- Accurate and up-to-date
- Retained only for as long as it is needed
- Kept securely

The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles". Beckfoot Trust are both a Data Controller and a Data Processer.

6. Accountability (DPO/Named GDPR Director)

Beckfoot Trust as a publicly funded organisation have to appoint a **Data protection officer (DPO),** this will be the **Trust Compliance Officer** will be the designated Data Protection Officer (DPO) and duties will include:

- Informing and advising the Trust and employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the Trust and Trust school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and ensuring the Trust and Trust employees receive appropriate training and data protection awareness communications.

The Trust Compliance Officer will update Beckfoot Trust Board on GDPR compliance, GDPR compliance will be overseen by the Trust Named **GDPR Director Paul Speight.**

7. Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed. **Processing** is the collection, recording, organisation structuring, storage, adoption or alteration, retrieval, consultation or use, disclosure, destruction or erasure of personal data.

Under the GDPR, data will be lawfully processed under the following conditions:

- **Legal Obligation** – The performance of a task for statutory/legal reasons.
- **Public Interest** - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- **Contractual Obligation** - For the performance of a contract with the data subject or to take steps to enter into a contract e.g. Staff Contracts.
- **Vital Interest** - Protecting the vital interests of a data subject or another person e.g. emergency medical situation.

- **Legitimate Interest** - 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.)
- **Consent** - Where processing cannot be categorised under the above conditions, the consent of the data subject **must** be held or obtained e.g. sharing photographs, news stories and individual examination results.

Special Categories of Data "Sensitive data" will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- 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 on the basis of Union or Member State 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 on the basis of Union or Member State law or a contract with a health professional.
- 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 Article 89(1).

8. Consent

Consent must be:	Consent, cannot be obtained from the following:
• Freely given (a positive indication) • Specific. • Informed. • An unambiguous indication of an individual's wishes. • A form of firm confirmation or positive opt-in, such as ticking boxes on a webpage. • Easily able to be withdrawn	• Silence • Pre-ticked boxes • Inactivity

*Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

Where consent is given, a record will be kept documenting how and when consent was given on student records and staff files or other storage mechanism. This information must be readily available for staff to check that consent has been obtained e.g. use of student photographs.

Beckfoot Trust and Trust schools must ensure that consent mechanisms meet the standards of the 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.

NOTE: Where processing is deemed to require "Consent", Beckfoot Trust and Trust Schools are aware that this "Consent" can be withdrawn by the individual at any time. It is therefore extremely important that schools consider any processing activities whereby data is shared or processed and becomes outside the control of Beckfoot Trust and Trust schools, in these instances, specific "informed" consent will need to be obtained.

Where a child is under the age of 16 [or younger if the law provides it (up to the age of 13)], the consent of parent/carer (person with legal responsibility)/legal guardian) will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

9. The right to be informed / Sharing Personal Data (Privacy Notices)

The GDPR requires us to inform individuals if we collect, process or share personal information about them. We are also required to share personal information about its staff or students with other organisations, mainly with the local authority, other schools and educational bodies, and potentially children's services and various contracted school services and systems.

We will issue Privacy Notices (also referred to as Fair Processing Notices) as outlined below. Copies can also be obtained on school websites and upon request from the school.

Beckfoot Trust adopt the DFE Model Privacy Notices for schools as the basis of our Privacy Notices and wherever possible will ensure that the privacy notice is written in a clear, plain manner.

- **Student Privacy Notices** will be built into School Admission Forms which are signed a the parent/carer (person with legal responsibility)/legal guardian) and the student where relevant upon entry to the school.
- **Staff Privacy Notices** will be issued with the Contract documentation.
- **Privacy Notices for "Other Individuals"** will be issued where necessary e.g. Board Member, Contractors, Volunteers, Visitors etc. where we will be processing their personal data.

10. The Right of Access

Individuals have the right to obtain confirmation that their data is being processed and the right to submit a data subject access request (DSAR) to gain access to their personal data in order to verify the lawfulness of the processing or obtain copies of their records for other purposes.

Trust staff should follow the **Trust Data Subject Access Request Procedure**. See Flowchart at **Appendix 2.**

The Trust website Data Protection and GDPR Page has guidance for individuals wishing to make a data subject access request.

11. The right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified and can do this through a request to Beckfoot Trust or relevant Trust school. Upon receiving a request for rectification, the Trust or Trust school should take the following action immediately:-

- check the validity of the request e.g. confirm identity of the person requesting the change.
- If the request is valid, amend the information where possible and record the actions taken.

- Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible. Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.
- Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
- Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

12. The right to erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the **right to erasure** in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

- **Where personal data has been disclosed to third parties**, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.
- **Where personal data has been made public within an online environment**, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

13. The right to restrict processing

Individuals have the right to block or suppress the Trust or Trust school's processing of personal data. Where a restriction may affect the Trust or Trust school carrying out their legal and contractual obligations or it is believed that the data is being processed under the Public Interest, Vital Interest or Legitimate Interest conditions of processing, guidance from the Trust Compliance Officer and/or the Information Commissioner's Officer to determine that the request is valid.

In the event that request is valid and the processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.
- If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
- The school will inform individuals when a restriction on processing has been lifted.

14. The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form.
The school will provide the information free of charge, and;

- Where feasible, data will be transmitted directly to another organisation at the request of the individual.
- The school is not required to adopt or maintain processing systems, which are technically compatible with other organisations.
- In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.
- The school will respond to any requests for portability within one month.
- Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.
- Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

15. The right to object

The school will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest

- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The school will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

16. Automated decision making and profiling

Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.
- The school will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, the school will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent/carer (person with legal responsibility)/legal guardian by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The school has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

17. Privacy by design and privacy impact assessments

The key aims of Privacy by Design are:-

- Proactive not reactive measures.
- Privacy as a default setting.
- Privacy embedded.
- Privacy throughout project life cycle.

The school will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures, which demonstrate how the Trust and Trust schools have considered and integrated data protection into their processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy. DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation, which might otherwise occur.

A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

Where a DPIA indicates high-risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

Trust employees should follow the **Trust Data Protection Impact Assessment (DPIA) Procedure –** see flowchart **Appendix 3**.

18. Data breaches

Trust employees should following the **Trust Data Breach Management Procedure** - see flowchart at **Appendix 4**.

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Please refer to the Trust Breach Management Procedure for further information.

Failure to report a breach when required to do so may result in a fine, as well as a fine of up to €20 million, or 4% of an organisations global turnover for the breach itself.

19. Third Party Processors/ Other authorised persons

The Trust requires all third party processors who have access to or process personal data on behalf of the Trust, to provide written confirmation that they will comply with the requirements of the GDPR and maintain adequate physical and IT security controls to protect our data.

We will request contractors, suppliers, and system providers who may process our personal data to written assurance provide contract terms to confirm that:-

- Any personal data you receive from us in the course of your performance of the relevant contract or service level agreement will only be processed in accordance with our documented instructions.
- No personal data will be transferred to any country outside the EEA or any international organisation without obtaining our prior written consent.

- Any of your employees, sub-contractors or other personnel who may be involved in the processing of the personal data are bound by written contractual obligations to keep the personal data confidential.
- No third party will be engaged to carry out any processing activities in respect of the personal data without our prior written consent, and if consent is given, the third party will be subject to a written contract containing the same data protection obligations as set out between you and us in the contract or service level agreement, and the provisions of this letter.
- Appropriate organisational and technical security measures are in place to protect any personal data, which may be processed or handled under the contract or service level agreement, and to assist us in complying with our obligations to deal with requests from data subjects to exercise their rights under the GDPR.
- Appropriate systems to investigate and report data breaches are in place and that all breaches will be notified to Beckfoot Trust immediately and the ICO within 72 hours (where relevant).
- You will assist us in complying with our obligations in relation to security of processing, dealing with data breaches and carrying out privacy impact assessments.
- When the services under the contract or service level agreement end, you will (at our option) delete or return all personal data and copies of the same.
- You will make information demonstrating compliance with the above obligations available to us on request and will allow for and contribute to any audits or inspections that we may conduct.

We will seek written confirmation from other authorised persons e.g. Candidates, Students, Volunteers, Contractors, Freelancers, Board Members, LSC Members that they will comply with Trust and Trust school policies and procedures and that we expect appropriate physical and IT data security controls to be exercised if given access to personal data and systems.

20. Data security

Beckfoot Trust will obtain and maintain Cyber Essentials Accreditation to demonstrate our IT Security Management Systems are effective.

Trust schools will ensure that the physical security of the school's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Beckfoot Trust, its employees and others with authorised access to personal data will ensure that appropriate IT and physical data security controls are used to protect unauthorised access to confidential records e.g.

1. Keep passwords secure, regularly change them and don't share with others?
2. Lock PC/Laptop screen or log off when away from your desk?
3. Position computer screens so they are not visible to "unauthorised persons" when in use.
4. Exercise caution when using Laptops in public areas and only connect to secure Wi-Fi connections?
5. Be aware of who can overhear sensitive conversations, take necessary precautions?
6. Operate a "Clear Desk Policy" and securely store papers/files that contain personal data when not in use.
7. Be careful when opening emails and attachments if you don't recognise the sender or the heading looks suspicious) or visiting new websites e.g. virus aware?
8. Dispose of personal data securely e.g. shred/confidential waste bin.
9. Encrypt or password protect personal information on attachments/devices/memory sticks?
10. Update personal data as soon as you are made aware of any changes e.g. notify the Admin/HR Team.
11. Ensure old devices/laptops/hard drives are given to IT/School Business Manager to dispose of securely.
12. Follow Trust Data Sharing Guidance and check there is a legal basis or that we hold a signed Privacy Notice or Data Subject Access Request before sharing personal information about staff and students (and others)?

13. Report breaches or potential breaches and fraudulent attempts to access data.

21. CCTV and photography

The Trust and Trust schools understand that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

CCTV

Trust staff will follow the Trust CCTV Policy for information in relation to the use and purpose of CCTV monitoring in Trust schools.

Photographs and non-CCTV recording images

The Trust will request consent for taking photographs and recording/videoing of students, staff and others and will only use them for the purposes covered on the appropriate Trust Privacy Notices. If the Trust or Trust schools require to use images for any other purpose, permission will obtained from the individual or for students, the parent/carer (person with legal responsibility/legal guardian) if under the age of consent.

Precautions will be taken, as outlined in the Trust Online Safety, ICT and Social Media Policy in relation to the taking and publishing photographs of students, in print, video or on the school website.

Images/Videos captured by individuals for recreational/personal purposes

For clarification, Images captured by individuals for recreational/personal purposes, and videos made by a parent/carer for family use, are exempt from the GDPR, however, the Trust and Trust schools do require that permission be obtained from the Trust/Trust school beforehand.

22. Data retention

Under the GDPR, Data must not be kept for longer than is necessary. It is therefore extremely important that the Trust and Trust schools have effective policies and procedures in place to ensure the timely secure disposal or deletion of data e.g. paper records disposed of via confidential waste bins and appropriate IT controls for electronic data.

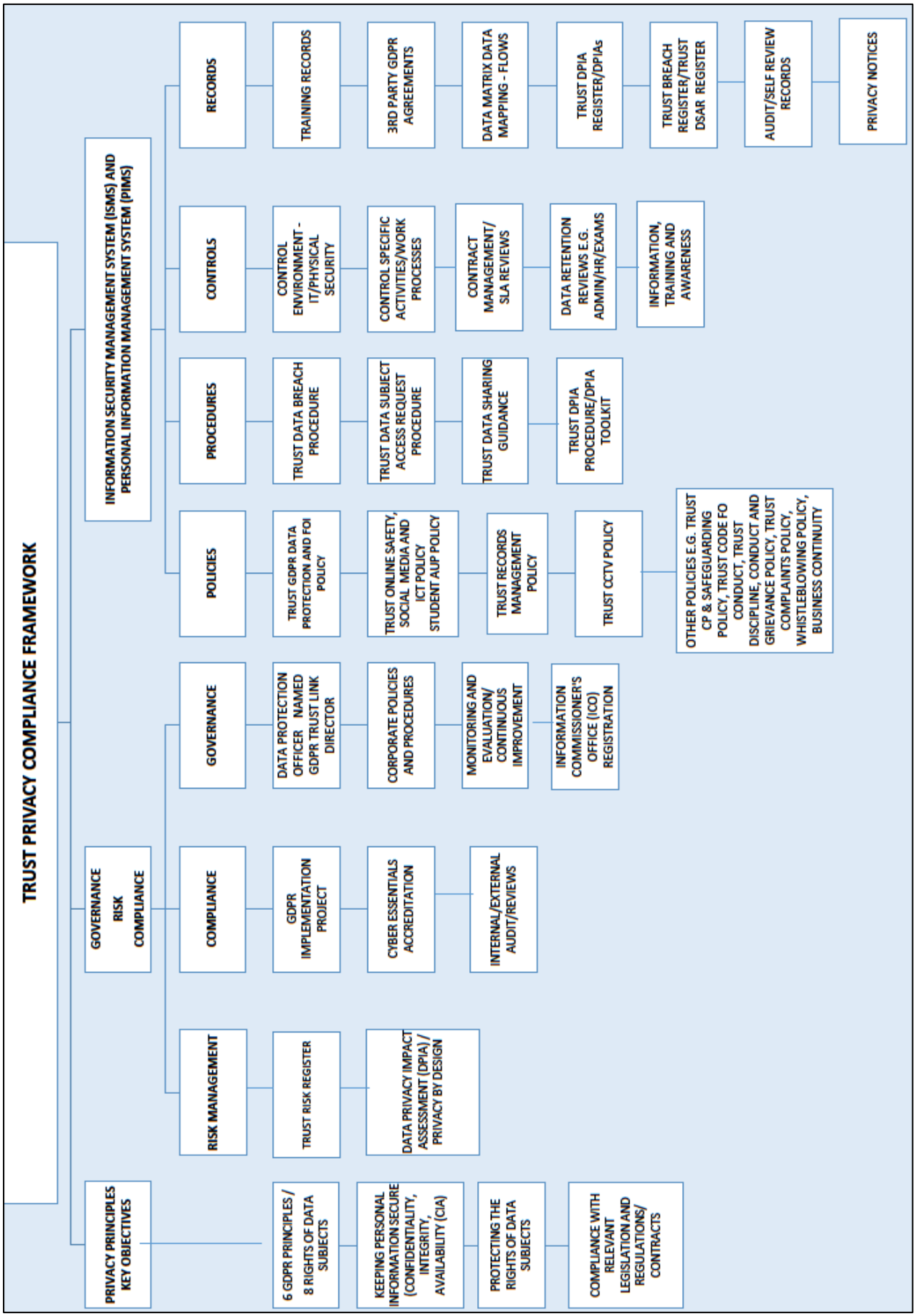
Some records relating to former students or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Trust employees will follow the guidance set out in the **Trust Records Management Policy**.

23. Policy review

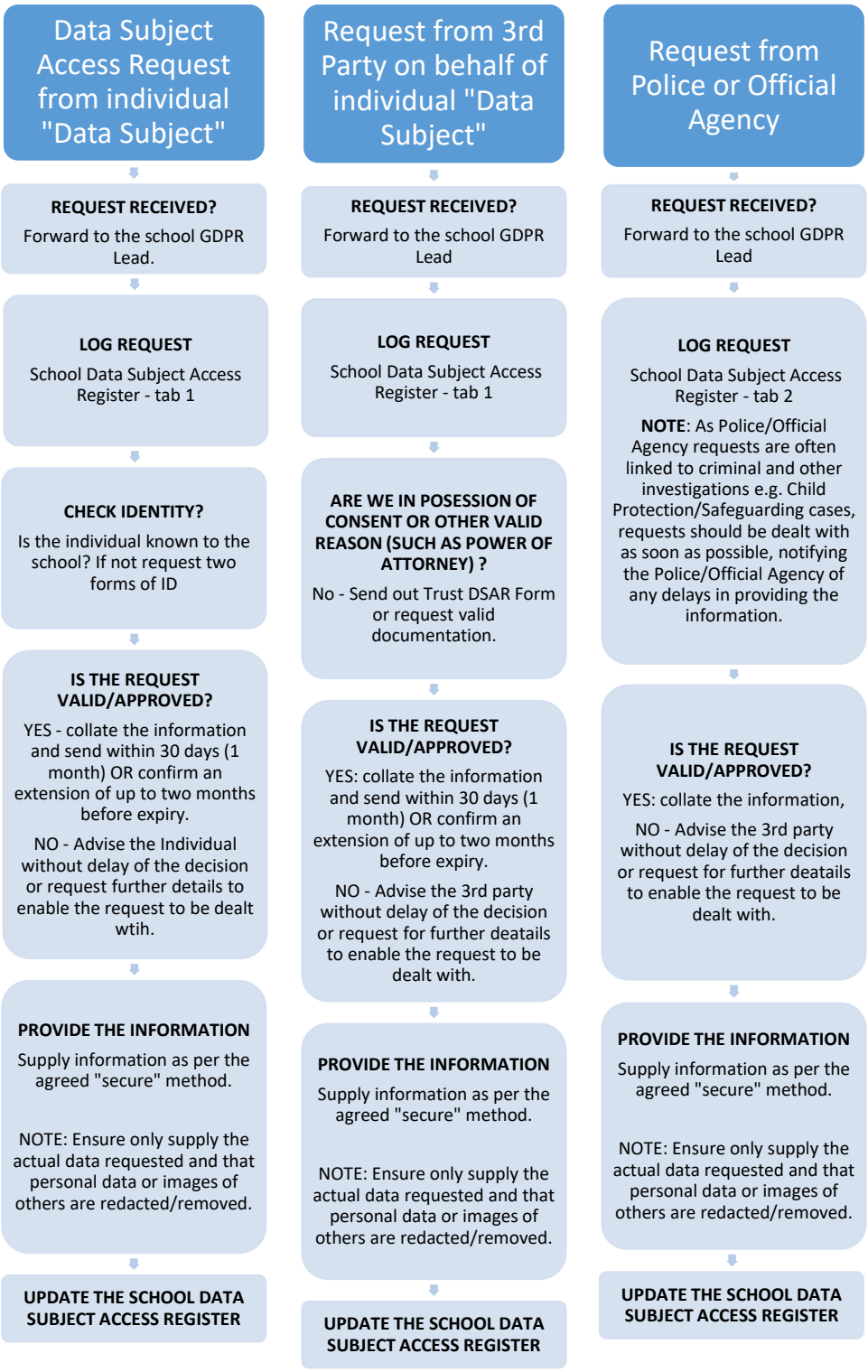
This policy is reviewed annually by the Trust Compliance Officer.

24. APPENDIX 1 - TRUST PRIVACY COMPLIANCE FRAMEWORK

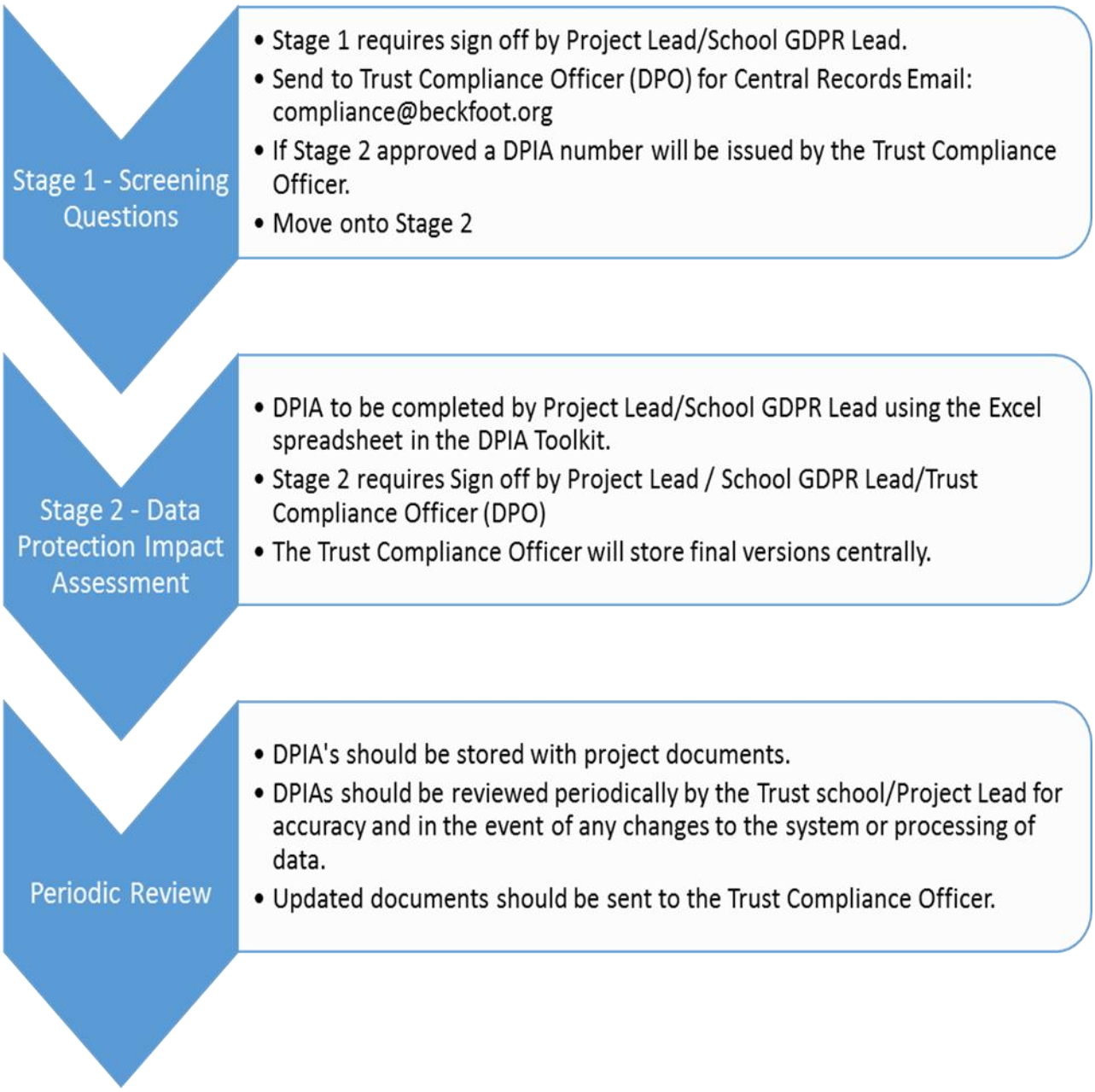


25. APPENDIX 2 – TRUST DATA SUBJECT ACCESS REQUEST PROCEDURE

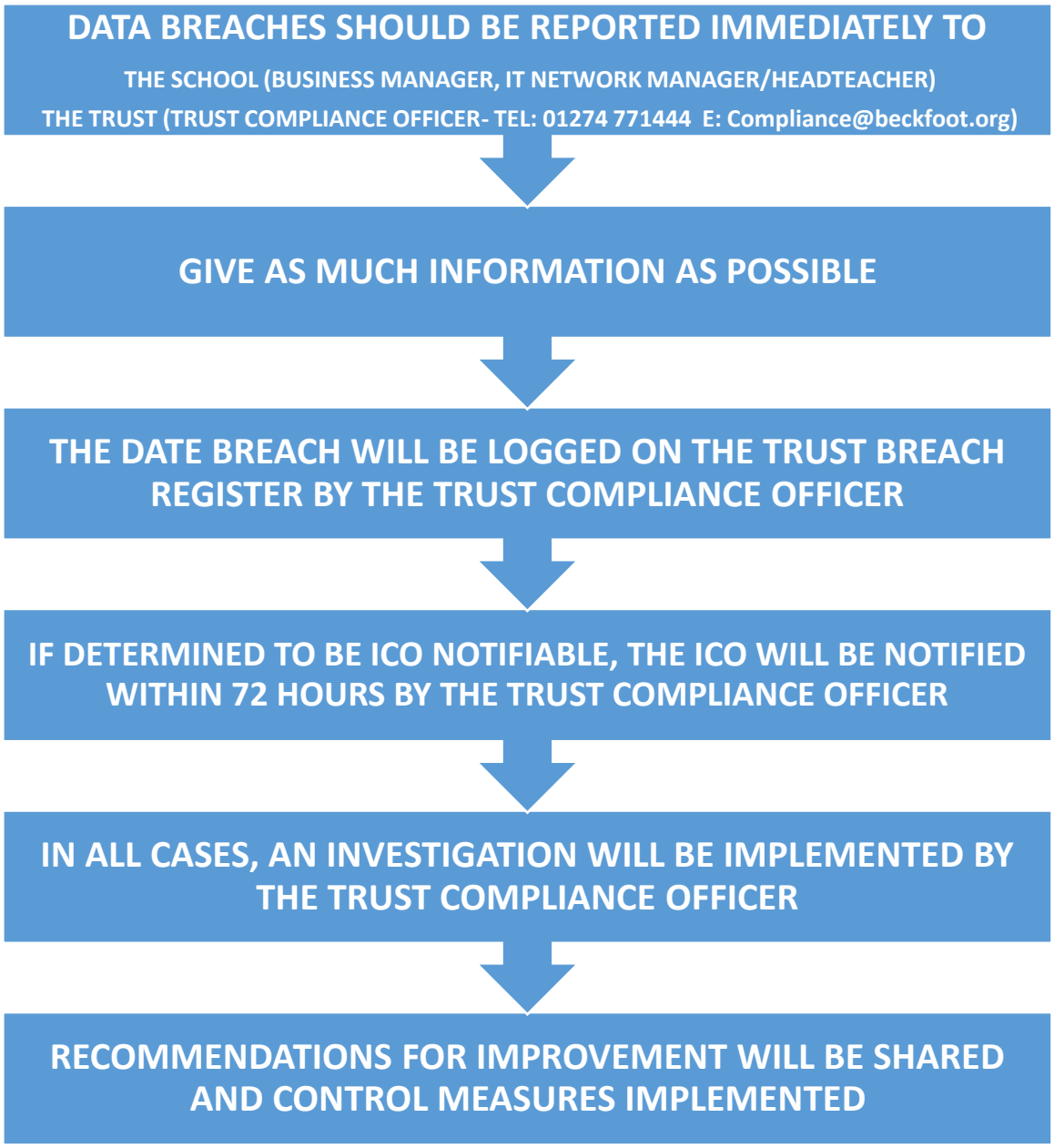
To be used in conjunction with Trust Privacy Notices and Trust Data Sharing Guidance



26. APPENDIX 3 - TRUST DPIA PROCEDURE FLOWCHART



27. APPENDIX 4 - TRUST DATA BREACH MANAGEMENT PROCEDURE



28. APPENDIX 4 - TRUST DATA PROTECTION – DATA SHARING GUIDANCE V1.2

Trust Data Protection – Data Sharing Guidance V1.2

To ensure that the sharing of Trust and school level data complies with the law the checklists below should be used in conjunction with the following policies and guidance:-

- Trust Data Protection and Freedom of Information Policy (Trust GDPR Data Protection and FOI Policy M ay 2018) and other policies e.g. CCTV Policy, Trust Social Media and ICT Policy, Trust Records Management Policy.
- Trust Data Subject Access Request Procedure
- Trust Data Protection Training
- Staff Privacy Notice (will be updated for May2018)
- Student Privacy Notice (will be updated for May 2018)
- Privacy Notice for "Others" (will be implemented for May 2018)
- ICO Data Sharing Code of Practice – search for latest version at www.ico.org.uk

Please forward Data Protection requests to the School Business Manager. Advice is available from the Trust Compliance Officer for complex requests.

DATA SHARING CHECKLISTS	
ONE OFF REQUESTS	**SYSTEMATIC DATA SHARING**
Example: You are asked to share personal data relating to a pupil, family members or member of staff in a 'one off' circumstance e.g. a parent asks for a copy of their child's education records or the school receives a request for data in relation to a criminal investigation. **KEY POINTS TO CONSIDER** **IS THE SHARING JUSTIFIED?** • Do you think you should share the information? • Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing? (e.g. SEN data/Child Protection details) • Have you assessed the potential benefits and risk to individuals and/or society of sharing or not sharing? • Do you have concerns that an individual is at risk of serious harm? • Do you need to consider an exemption in the DPA to share? **DO YOU HAVE THE POWER TO SHARE?** • Is the data outlined in the Student/Staff Privacy Notices and has consent been obtained? • The nature of the information you have been asked to share (for example was it given in confidence. E.g. Child Protection details – involved the school DSL). • Any legal obligation to share information (for example a statutory requirement or a court order e.g. Police Section 29 Request or Education Act – The law allows the transfer of pupil data when a child moves schools and to other agencies (as per Privacy Notice). **IF YOU DECIDE TO SHARE**	Example: You want to enter into an agreement to share staff or student personal data on an ongoing basis e.g. MIS Systems and systems//web platforms and apps which link to school MIS Systems or require manual uploads of staff and student data. A Data Protection Impact Assessment (DPIA) needs to be completed – see School Business Manager or IT Network Manager in first instance. **KEY POINTS TO CONSIDER** **IS THE SHARING JUSTIFIED?** • What is the sharing meant to achieve? • Have you assessed the potential benefits and risk to individuals and/or society of sharing or not sharing? • Is the sharing proportionate to the issue you are addressing? • Could the objective be achieved without sharing personal data? **DO YOU HAVE THE POWER TO SHARE?** Requests for systems to be linked to school pupil and staff data should be requested through the School Business Manager who can liaise with the school ICT lead and system supplier to ensure data protection security protocols are adequate. **IF YOU DECIDE TO SHARE** It is good practice to have a data sharing agreement in place. As well as considering the key

What information should you share?

- Only share what is necessary – e.g. redact information if it does not relate directly to individual named in the data request (data subject).
- Distinguish fact from fiction.

How should the information be shared?

- Information must be shared securely e.g. encrypted document/email or via www.gov.uk Secure Access S2S School transfer or BSO Dropbox. Seek advice if you are unsure.
- Ensure you are giving the data to the right person – always check the identity and source of requests.
- Consider whether it is appropriate/safe to inform the individual that you have shared their information.

Record the decision

All requests and decisions should be recorded on the school Data Protection Register as per the Trust Data Protection and Freedom of Information Policy.

points above, your data sharing agreement should cover the following issues:

- The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure that adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it?
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

Many reputable systems suppliers will incorporate a Data Sharing Protocol as part of their agreement; schools should make sure this is adequate.

Record the Data Sharing Agreement/Data Protection Impact Assessment

Copy Data Sharing Agreements/DPIAs should be stored with the contract paperwork.

TAKE CARE WHEN DEALING WITH STUDENT AND STAFF DATA

Personal data is an individual's name and any other piece of identifying information – see below for examples of personal data handled in schools.

- Address details
- SEN status
- Free School Meals eligibility
- Pupil Premium
- Educational levels and results (Inc. mock/practice exam papers/pieces of work with comments/feedback)
- Child Protection details
- Witness/Incident details
- Accident Records
- Photographs
- Staff Payroll/Salary information
- Staff Performance Management details

TOP TIPS TO KEEP DATA SAFE

- Documents containing personal data should be shredded or placed in Security Waste Consoles.
- Do not leave documents printing which contain personal data – see above for examples.
- If something personal is left on a printer or somewhere public, pass it to the School Business Manager.
- Take care when using electronic whiteboards in classrooms - registers often show FSM, SEN alerts etc.
- Parent evenings etc. take care not to inadvertently display other student's results/grades if using lists.
- Ensure you confirm the identity of callers and email addresses before discussing personal data.
- Where necessary to send data elsewhere, send it securely – see Data Protection Training for guidance.
- Keep your working area and desk tidy and do not leave documents lying around for others to see.
- Take care not to display personal data if visitors and students regularly use your office.
- Lock your PC/Laptop when not in use – especially in classrooms/public areas.
- Check the school holds signed Privacy Notices before sharing any data covered by the Privacy Notices.

Beckfoot Trust

29. Freedom of Information Introduction

1. Background
The Freedom of Information Act (FOIA) was introduced to promote greater openness and accountability across the public sector, and establishes a general right of access to information held by public authorities, including Academies. Along with Human Rights and Data Protection legislation, Freedom of Information (FOI) aims to build a culture of rights and responsibilities for citizens.

2. Right to request information
There is a legal right for any person to make a request to an Academy for access to information held by that Academy. Academies are under a duty to provide advice and assistance to anyone requesting information. Enquirers do not have to say why they want the information and the request does not have to mention FOIA.

The enquirer is entitled to be told whether the Academy holds the information (this is known as the duty to confirm or deny) and, if so, to have access to it. Access can include providing extracts of a document or a summary of the information sought, or access to the original document. However, the FOIA recognises the need to preserve confidentiality of sensitive information in some circumstances and sets out a number of exemptions. There are only four reasons for not complying with a valid request for information under FOI: -

1. the information is not held
2. the cost threshold is reached
3. the request is considered vexatious or repeated
4. one or more of the exemptions apply

3. Responsibility and delegation:
The Trust Board are responsible for the maintenance and review of this scheme and policy.
The Trust Board delegates the day-to-day responsibility for the FOIA policy and the provision of advice, guidance, publicity and interpretation of the Trust's policy to Trust Schools. Trust Schools will designate a staff member to act as a single point of reference, coordinate FOIA requests and apply related policies and procedures, take a view on possibly sensitive areas, ensure all staff are aware of the policy and consider what information and training staff may need.

Trust Schools should ensure that well managed records management and information system exists in order to comply with requests. Trust Schools should publish the Publication Scheme on the school website, the Publication Scheme is set out in Appendix A.
Copies of all requests, responses and refusals will be recorded by Trust Schools on a central register.

Trust Schools should ensure that requests are dealt with in accordance with 'The Freedom of Information Act 2000, a guide for Academies and Academy Trusts' which can be downloaded from www.gov.uk website.

4. How to request information
If you would like to make a request under the FOIA, please check the Publication Scheme on the Website initially, if the information is not available on the relevant school website please:

- make the request in writing (this includes email)
- state the enquirer's name and correspondence address (email addresses are allowed);

- describe the information requested - there must be enough information to be able to identify and locate the information.

You do not have to explain why you want the information or state that it is a FOI request, but it may help us to reply to your request more promptly if you let us know that it is a FOI request.
Requests for information should be addressed to: Trust Compliance Officer, Beckfoot Trust, Wagon Lane, Bingley. BD16 1EE or email: compliance@beckfoot.org.

5. Timeline for reply
We will do our upmost to reply to any request promptly. In any case, we will meet the legally prescribed limit of 20 working days, excluding non-school days. Where the 20th day to respond to a request is during a non-school day, we will have up to 60 days to respond e.g. summer holidays. The response time starts from the time the request is received. Where we need to ask you for more information to enable us to answer, the 20 days' start time begins when this further information has been received.
If a qualified exemption applies and we need more time to consider the public interest test, we will reply within the 20 days stating that an exemption applies and include an estimate of the date by which a decision on the public interest test will be made.
Where we have notified you that a charge is to be made, the time period stops until payment is received and then continues again once payment has been received.

6. Paying for information
The majority of information on the Publication Scheme will be freely available on the Trust or Trust school websites. We will aim to respond to FOI requests free of charge, however, if your request means that we incur significant costs e.g. a significant amount of photocopying, we will let you know the cost before fulfilling your request and charges will be as set out in the Schedule of Charges below.

7. Categories of information published
The publication scheme guides you to information which we currently publish (or have recently published) or which we will publish in the future. This is split into categories of information known as 'classes', see publication scheme at Appendix A.

8. Feedback and Complaints
To make any comments about this publication scheme and policy, for further assistance, or to make a complaint, please write to:
Trust Compliance Officer, Beckfoot Trust, Wagon Lane, Bingley. BD16 1EE.
If you are not satisfied with the assistance that you get or if we have not been able to resolve your complaint and you feel that a formal complaint needs to be made, then this should be addressed to the Information Commissioner's Office. This is the organisation that ensures compliance with the Freedom of Information Act 2000 and that deals with formal complaints. The complaint should be made in writing to:
The Case Reception Unit, Customer Service Team, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

30. Freedom of Information Publication Scheme

Below is a guide to information available from Beckfoot Trust and Trust schools as per the ICO Model Publication Scheme (Version 3 20130830 as at 21/07/2017).

Class 1 - Who we are and what we do (Organisational information, structures, locations and contacts). Current information only.		
Information to be published	**How information obtained**	**Cost**
Who's who in the school		

Who's who on the governing body / board of governors and the basis of their appointment	On request if not available on Trust or Trust school website.	For information not obtained via the website(s), a charge may be made as per the schedule of charges.
Instrument of Government / Articles of Association		
Contact details for the Head teacher and for the governing body, via the school (named contacts where possible).		
School prospectus (if any)		
Annual Report (if any)		
Staffing structure		
School session times and term dates		
Address of school and contact details, including email address.		
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). Current and previous financial year.		
Information to be published.	**How information obtained**	**Cost**
Annual budget plan and financial statements	On request if not available on Trust or Trust school website.	For information not obtained via the website(s), a charge may be made as per the schedule of charges.
Capital funding		
Financial audit reports		
Details of expenditure items over £2000 – published at least annually but at a more frequent quarterly or six-monthly interval where practical.		
Procurement and contracts the school has entered into, or information relating to / a link to information held by an organisation which has done so on its behalf (for example, a local authority or diocese).		
Pay policy		
Staff allowances and expenses that can be incurred or claimed, with totals paid to individual senior staff members (Senior Leadership Team or equivalent, whose basic actual salary is at least £60,000 per annum) by reference to categories.		
Staffing, pay and grading structure. As a minimum the pay information should include salaries for senior staff (Senior Leadership Team or equivalent as above) in bands of £10,000; for more junior posts, by salary range.		
Governors' allowances that can be incurred or claimed, and a record of total payments made to individual governors.		
Class 3 – What our priorities are and how we are doing (Strategies and plans, performance indicators, audits, inspections and reviews). Current information only.		
Information to be published.	**How information obtained**	**Cost**
School profile (if any) and in all cases: Performance data supplied to the English or Welsh Government or to the Northern Ireland Executive, or a direct link to the data The latest Ofsted / Estyn / Education and Training Inspectorate report - Summary - Full report - Post-inspection action plan	On request if not available on Trust or Trust school website.	For information not obtained via the website(s), a charge may be made as per the schedule of charges.
Performance management policy and procedures adopted by the governing body.		
Performance data or a direct link to it		
The school's future plans; for example, proposals for and any consultation on the future of the school, such as a change in status		

Safeguarding and child protection (Policy)		
Class 4 – How we make decisions (Decision making processes and records of decisions) Current and previous three years.		
Information to be published.	**How information obtained**	**Cost**
Admissions policy/decisions (not individual admission decisions) – where applicable	On request if not available on Trust or Trust school website.	For information not obtained via the website(s), a charge may be made as per the schedule of charges.
Agendas and minutes of meetings of the governing body and its committees. (NB this will exclude information that is properly regarded as private to the meetings).		
Class 5 – Our policies and procedures (Written protocols, policies, procedures for delivering our services and responsibilities) Current information only.		
Information to be published.	**How information obtained**	**Cost**
Records management and personal data policies, including: Information security policies Records retention, destruction and archive policies Data protection (including information sharing policies)	On request if not available on Trust or Trust school website.	For information not obtained via the website(s), a charge may be made as per the schedule of charges.
Charging regimes and policies.		
Class 6 – Lists and Registers Currently maintained lists and registers only (this does not include the attendance register).		
Information to be published.	**How information obtained**	**Cost**
Curriculum circulars and statutory instruments	On request if not available on Trust or Trust school website.	For information not obtained via the website(s), a charge may be made as per the schedule of charges.
Disclosure logs		
Asset register		
Any information the school is currently legally required to hold in publicly available registers		
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 - some information may only be available by inspection)		
Information to be published	**How information obtained**	**Cost**
Extra-curricular activities	On request if not available on Trust or Trust school website.	For information not obtained via the website(s), a charge may be made as per the schedule of charges.
Out of school clubs		
Services for which the school is entitled to recover a fee, together with those fees		
School publications, leaflets, books and newsletters		

31. Freedom of Information Schedule of Charges

The cost of providing information where indicated will be based as detailed below.

TYPE OF CHARGE	DESCRIPTION	BASIS OF CHARGE
Disbursement cost	Photocopying/printing @ ..p per sheet (black & white) @ ..p per sheet (colour)	Actual cost incurred by the school.
	Postage	Actual cost of Royal Mail standard 2nd class (or other class requested).
Statutory Fee		In accordance with the current legislation