'Innovative Education - Transforming Lives'

Freedom of Information and General Data Protection Policy

Status	Statutory
Responsible Directors	Directors Board
LGB	Full Governing Board
Responsible Persons	Mrs. B Nixon CEO
Date Policy Agreed	May 2018
Date of last review	September 2020
Date of next review	September 2022

Contents

Version Control

Version	***Revision Date***	***Revised by***	***Section Revised***
V2	29/5/2018	D Ashmore	All Sections
V2	29/7/2019	D Ashmore	All Sections no changes made
V2	30/09/2020	L Burton	Changed review dates on front of policy to reflect 2 year review stated in section 1
	22/01/2020	J Tuke	Pg 7 Replaced reference to Business and Operations Manager with Chief Operations Officer

1. Purpose

The purpose of this policy and procedure is to ensure compliance of the Exceed Learning Partnership Trust with all of its obligations as set out in the General Data Protection Regulation (GDPR) and Freedom of Information legislation.

Exceed Learning Partnership collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with the Trust or our academies in order to provide education and associated functions. The Trust may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with Genera Data Protection Regulation (GDPR) and other related legislation.

The GDPR applies to all computerized data and manual files if they come within the definition of a filing system. Broadly speaking, a filing systems is one where the data is structured in some way that is searchable on the basis of specific criteria (so you would be able to use something like the individual's name to find their information). If this is the case, it does not matter whether the information is located in a different physical location.

This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation and shall be reviewed every 2 years.

2. Data Controller

The Trust is the Data Controller as defined in the Data Protection Act 1998.

3. Notification with the Information Commissioner's Office (ICO)

3.1. The Trust notified the ICO, when it was established, using the on-line form http://www.ico.gov.uk/for_organisations/data_protection/notification/notify.aspx

3.2. Notification used the ICO template (N934) for a Trust.

3.3. The Trust will renew the registration annually. In addition, if the Trust or its Academies introduces new purposes for processing personal information, such as the installation of CCTV, then it will notify the ICO, be e-mail at **notification@ico.gsi.gov.uk,** requesting that the new purpose be included in the registration.

4 Definitions

4.1. **Personal data** is information that relates to an identifiable living individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain[1]. A subset of personal data is known as 'special category personal data'. This special category data is information that relates to:

4.1.1 Race or ethnic origin;

4.1.2 Political opinions;

4.1.3 Religious or philosophical beliefs;

4.1.4 Trade union membership;

4.1.5 Physical or mental health;

4.1.6 An individual's sex life or sexual orientation;

4.1.7 Generic or biometric data for the purpose of uniquely identifying a natural person

4.2 Special Category information is given special protection, and additional safeguards apply if this information is to be collected and used.

4.3 Information relating to criminal convictions shall only be held and processed where there is a legal authority to do so.

4.4 The Trust does not intend to seek or hold sensitive personal data about staff or pupils except where the Trust has been notified of the information, or it comes to the Trust's attention via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with the legal obligation or as a matter of good practice. Staff or pupils are under no obligation to disclose to the Trust their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements).

5. Data Protection Principles

[1] For example, if asked for the number of male employees, and you only have one male employee, this would be personal data if it was possible to obtain a list of employees from the website

5.1 The six core principles as laid down in the GDPR are followed in this policy in the Trust's commitment that personal data:

- Is processed fairly, lawfully and in a transparent way, and processing shall not be lawful unless one of the processing conditions can be met;

- Personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be processed further in a manner incompatible with those purposes;
- Personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;
- Personal data shall be accurate and where necessary kept up to date;
- Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes;
- Personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures;

5.2 In addition to this the Trust is committed to ensuring that at all times anyone dealing with personal data shall be mindful of the individual's right under the law (as explained in more details 5.3 below)

5.3 The Trust is committed to complying with the principles in 5.1 at all times. This means that the Trust will:

- Inform individuals as to the purpose of collection any information from them as and when we ask for it;
- Be responsible for checking the quality and accuracy of the information
- Regular review our records held to ensure that information is not held longer than necessary and that it has been held in accordance with the data retention policy;
- Ensure that information authorized for disposal it is disposed of securely i.e. shredded
- Ensure appropriate security measures to safeguard personal information whether it is held in paper format or electronically and follow the relevant security policy requirements at all times;
- Share personal information with others only when it is necessary and legally appropriate to do so;
- Set clear procedures for responding to request for access to personal information known as a 'subject access request';
- Report any breaches of GDPR in accordance with the procedures set out in section 19 below

6 Conditions for processing in the first data protection principle

6.1 The Trust holds personal data on students, staff and other individuals such as visitors. In each case, the personal data must be treated in accordance with the data protection principles as outlined in paragraph 5.1 above

Pupils Privacy Notice

6.2 The personal data held regarding students includes contact details, assessment / examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.

6.3 The data is used in order to support the education of the students, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the academy as a whole is doing, together with any other uses normally associated with this provision in an academy environment.

6.4 In particular the Academy may but is not exhaustive:

6.4.1 Transfer information to any provider, society or club set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotion purpose relation to the academy but only where consent has been obtained in the first instance;

6.4.2 Make personal information, including sensitive personal information, available to staff for planning curricular or extra-curricular activities;

6.4.3 Use photographs of pupils in accordance with the photograph policy

6.5 Any wish to limit or object to any use of personal data a request for a Parental Consent Withdrawal Form should be requested from your Academy Chief Privacy Officer. If in view of the Academy Principal, the objection cannot be maintained the individual will be given reasons why in writing outlining why the academy cannot comply with their request;

Workforce Privacy Notice

6.6 The personal data held about staff will include contact details, employment history, bank details, national insurance number, career progression, DBS checks, photographs, special categories including information such as gender, age and ethnic group. The Trust may pass information to other regulatory authorities where appropriate and may use names and photographs of staff in publicity and promotional flyers.

6.7 Staff should note that information about disciplinary action may be kept for longer than duration of the sanction. Although treated as “spent” once the period of the sanction has expired, the details of the incident may need to be kept for longer period.

6.8 Any wish to limit or object to the use to which personal information is to be put should be notified to the Trusts Chief Operations Officer who will ensure that this is recorded, and adhered to if appropriate. If the Chief Operations Officer is of the view that it is not

appropriate the individual will be given written reasons why the Trust cannot comply with their request.

Other individuals

6.9 The Trust may hold personal information in relation to volunteers, supply staff and governors/directors. Such information shall be held only in accordance with the data protection principles and shall not be kept longer than is necessary.

7 Security of personal information

7.1 The Trust will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this Policy and their duties under the GDPR. The Trust will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

8 Disclosure of personal information to third parties

8.1. The following list includes the most usual reasons that the Trust will authorise disclosure of personal data to a third party:

8.1.1. To give a confidential reference relating to a current or former employee, volunteer or student;

8.1.2. For the prevention or detection of crime;

8.1.3. For the assessment of any tax or duty;

8.1.4. Where it is necessary to exercise a right or obligation conferred or imposed by law upon the Trust (other than an obligation imposed by contract);

8.1.5. For the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);

8.1.6. For the purpose of obtaining legal advice;

8.1.7. For research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);

8.1.8 To disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of academy trips;

8.1.9 To provide information to another educational establishment to which a pupil is transferring;

8.1.10. To provide information to the Examination Authority as part of the examination process; and to provide information to the relevant Government Department concerned with national education. At the time of the writing of this Policy, the Government Department concerned with national education is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

8.2 The DfE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified

from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.

8.3 The Trust may receive requests from third parties (i.e. those other than the data subject, the Trust, and employees of the Trust) to disclose personal data it holds about pupils, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or the Trust.

8.4 All requests for the disclosure of personal data must be sent to the Academy Chief Privacy Officer or the Trusts Data Protection Officer, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

9. Why do we collect information?

The Trust/Academies collects information about our pupils, employees and other individuals and holds this personal data so that we can:

- Support each pupil's learning;
- Monitor and report on each pupil's progress;
- Provide appropriate pastoral care and other support to each of our pupils;
- Assess how well each pupil is doing and report on that to the parents.
- Employment purposes
- To enable the development of a comprehensive picture of the workforce and how it is deployed
- To inform the development of recruitment and retention policies
- To assist in the running of the Trust and its academies
- To enable individuals to be paid

9.1. Do we share this information with anyone else?

We do not share any of this data with any other organisation without your permission except where the law requires it. We are required to provide pupil data to central government through the Department for Education (DfE) www.education.gov.ukand the Education Funding Agency (EFA) www.education.gov.uk/efa

Where it is necessary to protect a child, the Trust will also share data with the Local Authority Children's Social Services and/or the Police.

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

9.2.1. All pupils have a right to have a copy of the personal information held about them. As our pupils are of primary school age, a request for a copy of the personal information has to be made by a parent or guardian in writing. The only circumstances under which the information would be withheld would be if there was a child protection risk, specifically:

9.2.2. The information might cause serious harm to the physical or mental health of the pupil or another individual;

9.2.3. Where disclosure would reveal a child is at risk of abuse;

9.2.4. Information contained in adoption or parental order records;

9.2.5. Information given to a court in proceedings under the Magistrate's Courts (Children and Young Persons) Rules 1992; and

9.2.6. Copies of examination scripts.

9.2.7. 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, the information will be collected and provided within 30 calendar days.

10. Information Security

10.1. Objective

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

10.2. Responsibilities

The CEO of the Trust has direct responsibility for maintaining the Information Security policy and for ensuring that the staff of the Trust adheres to it.

The Principals of each academy are responsible for the implementation of this policy.

10.3. General Security

10.3.1. 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:

10.3.2. Not reveal building entry codes or any identifiable codes relating to their identity to allow people that you do not know or who cannot prove themselves to be employees;

10.3.3. Beware of people tailgating you into the building or through a security door;

10.3.4. 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;

10.3.5. Not position monitors/screens on reception desks where members of the public could see them;
10.3.6. Lock secure areas when you are not in the office;

10.3.7. Not let anyone remove equipment or records unless you are certain who they are;

10.3.8. Visitors and contractors in Trust buildings should always sign in a visitor's book which must be kept out of view of visitors to the buildings.

10.4. Security of Paper Records

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

10.4.2. 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;

10.4.3. Always keep track of files and who has them;

10.4.4. Do not leave files out where others may find them;

10.4.5. Where a file contains confidential or sensitive information, do not give it to someone else to look after.

10.5. Security of Electronic Data

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

10.5.2. Prevent access to unauthorised people and to those who don't know how to use an item of software properly. It could result in loss of information;

10.5.3. Keep suppliers CDs containing software safe and locked away. Always label the CDs so you do not lose them in case they need to be re-loaded;

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

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

10.5.6. Don't write it down;

10.5.7. Don't give anyone your password;

10.5.8. Your password should be at least 8 characters;

10.5.9. The essential rules your password is something that you can remember but not anything obvious (such as password) or anything that people could guess easily such as your name;

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

10.5.11. Include numbers as well as letters in the password;

10.5.12. Take care that no-one can see you type in your password;

10.5.13. Change your password regularly, and certainly when prompted. Also change it if you think that someone may know what it is.

10.5.14. 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.

10.5.15. Data must not be stored on desk tops or my document folders, where documents are being worked in draft form it is important they are moved to the network ASAP. Personal Data must not be stored on desk tops or my document folders.

10.6. Use of E-Mail and Internet

10.6.1. 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 web sites 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 Principal will ensure that the sites are reported to the broadband provider for filtering.

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

10.6.3. Do not send highly confidential or sensitive personal information via e-mail;

10.6.4. Save important e-mails immediately;

10.6.5. Unimportant e-mails should be deleted straight away;

10.6.6. Do not send information by e-mail, which breaches the General Data Protection Regulation. Do not write anything in an e-mail which could be considered inaccurate or offensive, and cannot be substantiated.

10.7. Electronic Hardware

10.7.1. All hardware held within Trust should be included on the asset register;

10.7.2. When an item is replaced, the register should be updated with the new equipment removed or replaced;

10.7.3. Do not let anyone remove equipment unless you are sure that they are authorized to do so;

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

10.8. Homeworking Guidance

10.8.1. If staff must work outside of the Trust or at home, all of the 'Information Security' policy principles still apply. However, working outside of the Trust presents increased risks for securing information. The following additional requirements apply:

10.8.2. Do not access confidential information when you are in a public place, such as a train and may be overlooked;

10.8.3. 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;

10.8.4. If you use a laptop or tablet or smart phone

10.8.4.1. Ensure that it is locked and pass-word protected to prevent unauthorised access;

10.8.4.2. 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;

10.8.4.3. 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 devise without the express permission of the Principal. Taking personal data off-site on a devise or media that is not encrypted would be a disciplinary matter;

10.8.4.4. The Principal will maintain a register of: protected data that has been authorised for use on a portable devise; the fixed period of time that the authorisation relates to; the reason why it is necessary to place it on the devise; the person who is responsible for the security of the device and its data; the nature of encryption software used on the devise; confirmation of the date that the data is removed from the devise.

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

10.8.6. If you are using your own computer, ensure that others cannot access documents. When you have completed working on them, transfer them back to the Trust's system and delete them from your computer. It is forbidden to use a computer owned by you to hold personal data about pupils or staff at the Trust.

10.9. Audit of Data Access

10.9.1. 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.

10.10. Data Backup

10.10.1. The Trust will arrange that all critical and personal data is backed up to secure on-line (off physical site) storage. If the Trust is physically damaged critical data backups will allow the Trust to continue its business at another location with secure data. Data saved on desk top, my documents or C: drive is not back up.

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

11. Disposal of Information

11.1. 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.

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

11.3. 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.

11.4. Where a third party contractor holds personal information on behalf of the Trust, for example a payroll provider, the Trust will seek reassurance from the contractor regarding their data protection policies and procedures.

12. Subject Access Requests

12.1. 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.

12.2. Trust staff may have access to their personal data within 30 days of a request and at no charge.

12.3. 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

13. Sharing of Personal Information

13.1. 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.

13.2. The Trust is required, for example, to share information with the Department for Education and the Education Skills 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.

13.3. Because our pupils are of primary school age, their own right to access their own personal information held by the Trust will be exercised through their parents or guardians.

13.4. The CEO/Principal will be responsible for authorising the sharing of data with another organisation. The CEO/Principal, in authorising the sharing of data will take account of:

13.5. Whether it is lawful to share it;

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

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

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

13.9. 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.

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

13.11. 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.

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

13.13. If consent has been obtained to share data which is not a legal requirement to do so.

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, is placed on the web site the following principles will apply:

14.3. We will not disclose personal information (including photos) on a web site without the consent of the pupil, parent, member of staff or Governor as appropriate;

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

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

15. CCTV

If the Trust uses CCTV this will be 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 General Data Protection Regulation, consent from parents, employees or individuals must be received.

16. Photographs

16.1. The Trust may only use photographs of pupils or staff taken for inclusion in the printed prospectus or other school publications where specific consent has been provided.

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

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

17. Processing by Others

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 have to specify how they will ensure compliance with general data protection regulations.

18. Training

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

19. Breach of any requirement under GDPR

19.1 Any breach of data protection must be reported immediately to the Chief Privacy Officer for your Academy, providing as much detail on the breach as possible I.e. when did it take place, what data has been breached, what actions you have taken to rectify the breach.

19.2 Once notified, the Chief Privacy Officer shall assess:

- The extent of the breach;
- The risks to the data subjects as a consequence of the breach;
- Any security measures in place that will protect the information;
- Any measures that can be taken immediately to mitigate the risk to the individual(s)
- Report breaches to the Data Protection Officer in the Trust;

19.3 Unless the Data Protection Officer concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioners Office within 72 hours of the breach having come to the attention of the Trust unless a delay can be justified.

19.4 The Information Commissioner will be told:

- Details of the breach, including the volume of data at risk, and the number of categories of data subjects;
- The contact point for any enquiries (Which shall be the Data Protection Officer);
- The likely consequences of the breach;
- Measures proposed or already taken to address the breach.

19.5 If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Data Protection Officer shall notify data subjects of the breach without undue delay unless data would be unintelligible to those not authorized to access it, or measures have been taken to mitigate any risk to the affected individuals.

19.6 Data Subjects shall be told:

- The nature of the breach;
- Who to contact with any questions;
- Measures taken to mitigate any risks

19.7 The Data Protection Officer shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the Accounting Officer and a decision made about implementation of those recommendations.

20. Glossary of relevant legislation

- The General Data Protection Regulation 2018
- The Freedom of Information Act 2000
- The Environmental Information Regulations 1992
- The Human Rights Act 1998
- The Regulation of Investigatory Powers Act
- Copyright and Intellectual Property rights
- The Computer Misuse Act

21. Freedom of Information Publication Scheme

Exceed Learning Partnership Multi Academy Trust Board is responsible for maintenance of this scheme.

1. Introduction: what a publication scheme is and why it has been developed

One of the aims of the Freedom of Information Act 2000 (which is referred to as FOIA in the rest of this document) is that public authorities, including academies, should be clear and proactive about the information they will make public.

The scheme covers information already published and information which is to be published in the future. All information in our publication scheme is either available for you on our website to download and print off or available in paper form.

Some information which we hold may not be made public, for example personal information. This publication scheme conforms to the model scheme for schools approved by the Information Commissioner.

2. 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'. The classes of information that we undertake to make available are:

Who we are and what we do

- Organisational information
- locations and contacts
- constitutional and legal governance.

What we spend and how we spend it

- Financial information relating to projected and actual income and expenditure
- tendering, procurement and contracts.

What our priorities are and how we are doing

- Strategy and performance information
- Plans
- Assessments
- inspections and reviews.

How we make decisions

- Policy proposals and decisions.
- Decision making processes
- internal criteria and procedures, consultations.

Our policies and procedures

- Current written protocols for delivering our functions and responsibilities.

Lists and registers

Information held in registers required by law and other lists and registers relating to the functions of the authority.

The services we offer
Advice and guidance, booklets and leaflets, transactions and media releases. A description of the services offered.

The classes of information will not generally include:
• Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.

• Information in draft form.

• Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons.

3. How information published under this scheme will be made available

Exceed Learning Partnership will indicate clearly to the public what information is covered by this scheme and how it can be obtained. Where it is within the capability of Trust and it's Academies, information will be provided on our website(s). Where it is impracticable to make information available on a website or when an individual does not wish to access the information by the website, we will indicate how information can be obtained by other means and provide it by those means. In exceptional circumstances, some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale .

Information will be provided in the language in which it is held or in such other language that is legally required. Where an authority is legally required to translate any information, it will do so.

Obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats will be adhered to when providing information in accordance with this scheme

4. Charges which may be made for information published under this scheme

The purpose of this scheme is to make the maximum amount of information readily available at minimum inconvenience and cost to the public. Charges made by the school for routinely published material will be justified and transparent and kept to a minimum. Material which is published and accessed on a website will be provided free of charge. Charges may be made for information subject to a charging regime specified by Parliament.
Charges may be made for actual disbursements incurred such as:

- photocopying
- postage and packaging
- the costs directly incurred as a result of viewing information

Charges may also be made for information provided under this scheme where they are legally authorised and they are in all the circumstances, including the general principles of the right of access to information held by public authorities, justified and are in accordance with a published schedule or schedules of fees which is readily available to the public. If a charge is to be made, confirmation of the payment due will be given before the information is provided. Payment may be requested prior to provision of the information.

5. Written requests

Information held by a public authority that is not published under this scheme can be requested in writing, when its provision will be considered in accordance with the provisions of the Freedom of Information Act.

6. How to request information

If you require a paper version of any of the documents within the scheme, please contact the school by telephone, email or letter. Contact details are set out below**,** or you can visit our website www.exceedlearningpartnership.co.uk or each academy website. To help us process your request quickly, please clearly make any correspondence "Publication Scheme Request".

Email: admin@hilltop.doncaster.sch.uk
Tel: 01709 863273
Address: Exceed Learning Partnership Trust,
Edlngton Lane, Edlington, Doncaster, DN12 1PL

7. Feedback and Complaints

We welcome any comments or suggestions you may have about the scheme. If you want to make any comments about this publication scheme or if you require further assistance or wish to make a complaint then initially this should be addressed to Chief Executive Officer, Exceed Learning Partnership, Edlngton Lane, Edlington, Doncaster, DN12 1PL

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 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. They can be contacted at:
Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Or

Enquiry/Information Line: 01625 545 700
E Mail: publications@ic-foi.demon.co.uk
Website: www.ico.gov.uk

Policy Agreed: Signed: CEO:
Signed: Chair of Directors:

Policy to be reviewed in autumn 2022

Freedom of Information Publication Scheme

In line with the Freedom of Information Act the academy will provide its Approved Publication Scheme on our web site.

Information to be published.	**How the information can be obtained**	**Cost**
Class 1 - Who we are and what we do (Organisational information, structures, locations and contacts) This will be current information only		
Who's who in Exceed Learning Partnership MAT board - names, role, register of interest, attendance, date of appointment	Trust website	
School staff and structure – names of key personnel	Academy website	free
Who's who on the governing body / board of governors and the basis of their appointment	Academy/Trust website	free
Instrument of Government / Articles of Association	Trust website	free
Contact details for the Principal and governing body, via the school (named contacts where possible).	Academy/Trust Website	free
School prospectus (if any)	Hard copy	free
Staffing structure	Academy Website/hard copy	free
School session times and term dates	Academy Website/hard copy	free
Address of school and contact details, including email address.	Academy Website/hard copy	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) Current and previous financial year as a minimum		
Annual budget plan and financial statements	Hard copy	10p per sheet
Capital funding	Hard copy	10p per sheet
Financial audit reports	Hard copy	10p per sheet

Procurement and Projects	Hard copy	10p per sheet
Pay policy	Hard copy/website	10p per sheet
Staffing and grading structure	Hard copy	10p per sheet
Class 3 – What our priorities are and how we are doing (Strategies and plans, performance indicators, audits, inspections and reviews) Current information as a minimum		
Academy profile (if any) • Government supplied performance data • Government Supplied Data The latest Ofsted Report	 Academy Website Academy Website	 free free
Performance management policy and procedures adopted by the governing body.	Hard copy	free
Safeguarding and child protection	Trust/Academies Website	free
Class 4 – How we make decisions (Decision making processes and records of decisions)		
Admissions policy/decisions (not individual admission decisions) – where applicable	Academies Website	free
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).	Hard copy	10p per sheet

Class 5 – Our policies and procedures (Current written protocols, policies and procedures for delivering our services and responsibilities) Current information only.		
• Charging and Remission Policy • Health and Safety • Staff Code of Conduct • MAT board Code of Conduct • Discipline and Grievance Policy • Equality and Diversity • Pupil and curriculum policies, e.g. SEND, accessibility	Trust Website Trust Website Trust Website Trust Website Trust Website Trust Website Academy Website	Free Free Free Free Free Free free
Records management and personal data policies, including: • Information security policies • Records retention, destruction and archive policies • Data protection (including information sharing policies)	Trust/Academy Website	free
Class 6 – Lists and Registers Currently maintained lists and registers only (**this does not include the attendance register)** (some information may only be available by inspection)		
Curriculum circulars and statutory instruments	Academy Website/Newsletter	Free
Disclosure logs	Hard copy	10p sheet
Asset register	Hard copy	10p sheet
Any information the school is currently legally required to hold in publicly available registers **(THIS DOES NOT INCLUDE THE ATTENDANCE REGISTER)**	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 (some information may only be available by inspection)		
Extra-curricular activities	Academy Website/School Office	free
Out of school clubs	Academy Website/School Office	free
Services for which the school is entitled to recover a fee, together with those fees	Hard copy	free
School publications, leaflets, books and newsletters	Academy Website/Hard copy	free

* the actual cost incurred by the public authority *Type of charge*	*Description*	*Basis of charge*
Disbursement cost	Photocopying/printing @ 10p per sheet (black & white)	Actual cost *
Postage	Actual cost of Royal Mail standard second class	