Data Protection and Freedom of Information (FOI) Policy

Key Manager	Trust Governance Manager
Ratified by BT	June 2018
Review Dates:	Spring 2023
Location of Policy:	Trust wide
Access to Policy:	Open
Policy Context:	This Policy applies to all staff of the Trust and to those others offered access to such resources.

Revision History

Revision Date	**Description**	**Sections Affected**	**Revised By**	**Approved By**
16/10/2018	Annual review	Whole policy and Trust references	H R Director	H R Committee
Spring 2020	Change DPO details			
Spring 2020	Review of policy following change of DPO advisor	Whole policy and Trust references	Trust Governance Manager & DPO	
Spring 2021	Annual review Northamptonshire County Council changes to North Northamptonshire Council All references to UK-GDPR changed to (UK) UK-GDPR in response to Brexit Clarity regarding who manages FOI requests Referenced GDPR leads in each school	Section 6 of FOI section Throughout the policy Section 5.3	Trust Governance Manager & DPO	
Spring 2023				

Contents

1. Aims

The Nene Education Trust ("the Trust") collects and uses personal data about staff, pupils, parents/carers, governors, trustees, visitors, volunteers and other individuals. The Trust may be required by law to collect and use certain types of information to comply with statutory obligations. This policy aims to ensure that data is collected, stored and processed in accordance with the The United Kingdom General Data Protection Regulation (UKGDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data regardless of whether it is paper or electronic format. Filing is defined where data is structured and searchable on the basis of specific criteria (such as a person's name).

2. Legislation and guidance

This policy meets the requirements of the UKGDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on UKGDPR and the ICO's guidance.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-GDPR/

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with the Trust's funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual and includes details that would identify an individual to the person to whom it is disclosed because of special knowledge that they have or can obtain[1] A subset of personal data known as "special category personal data".
Special category data	Special category personal data may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as username • Race or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Physical or mental health • An individual's sex life or sexual orientation • Genetic or biometric data for the purpose of uniquely identifying a natural person This type of data is given special protection, and additional safeguard

[1] An example could be, if asked for the number of female employees, and the Trust only has one female employee, tis would be personal data if it was possible to obtain a list of employees from the website

	apply if this information is to be collected and used. Information relating to criminal convictions will only be held and processed where there is legal authority to do so. The Trust does not intend to seek or hold Special Category Data about staff and pupils, except where the Trust has been notified of the information, or it comes to the Trust's attention via legitimate means or needs to be sought and held in compliance with legal obligations or as a matter of good practice. Staff and 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 the sexual life (other than the details of their marital status and or parenthood are needed for other purposes e.g. Pension entitlements)
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data Subject	The identified or identifiable individual whose personal data is held or processed
Data controller	A person or organisation (for example the Trust) that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

The Nene Education Trust processes personal data relating to parents/carers, pupils, staff, governors, trustees, visitors and others, and therefore is a data controller.

The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by the Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Board of Trustees

The Board of Trustees has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Trust board and, where relevant, report to the board their advice and recommendations on data protection issues for the Trust and its schools.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Nene Education Trust's Data Protection Officer: Angela Corbyn dpo@neneeducationtrust.org.uk or Tel: 07775 436141.

Within the Trust's Central team, general UK-GDPR queries are dealt with by Emma Morehen, Governance Manager who can be contacted via email: emma.morehen@neneeducatontrust.org.uk or Tel: 01933 627082

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis. Each School has a designated GDPR lead acting as link between the school, Trust Central Team and DPO regarding GDPR related matters.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;
    - If they have any concerns that this policy is not being followed;
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way;

- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area;
- If there has been a data breach;
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
- If they need help with any contracts or sharing personal data with third parties.

6. Data protection principles

The UKGDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed;
- Accurate and, where necessary, kept up to date;
- Kept for no longer than is necessary for the purposes for which it is processed;
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the school aims to comply with these principles.

- Personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

In addition to this, the Trust is committed to ensuring that at all times, anyone dealing with personal data will be mindful of the individual's rights under the law (as explained in more detail in paragraphs 7 and 8 below).

7. Collecting and processing personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract;
- The data needs to be processed so that the Trust can **comply with a legal obligation;**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life;
- The data needs to be processed so that the Trust, as a public authority, can perform a task **in the public interest,** and carry out its official functions;
- The data needs to be processed for the **legitimate interests** of the Trust or a third party (provided the individual's rights and freedoms are not overridden);

- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**.

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent;**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law;**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent;
- The data has already been made **manifestly public** by the individual;
- The data needs to be processed for the establishment, exercise or defence of **legal claims;**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation;
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law;
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law;
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent;**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent;
- The data has already been made **manifestly public** by the individual;
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights;**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law which will be shared in the relevant privacy notice

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done with reference to the Information and Records Management Society's toolkit for schools and the Trust's Retention Policy

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff or child at risk;
- We need to liaise with other agencies – we will seek consent as necessary before doing this;
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share;
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests (SARs) and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust holds about them. This includes:

- Confirmation that their personal data is being processed;
- Access to a copy of the data;
- The purposes of the data processing;
- The categories of personal data concerned;
- Who the data has been, or will be, shared with;

- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period;
- The source of the data, if not the individual;
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual;
- The right to lodge a complaint to the Information Commissioners Office (ICO);
- Where the personal data are not collected from the individual, any available information as to their source;
- Details of the safeguards in place for any transfers of their data to locations outside the European Economic Union.

Subject access requests can be submitted verbally or in writing to the Trust or the Trust's DPO. The Trust and DPO will need to clarify:

- Name of individual;
- Correspondence address;
- Contact number and email address;
- Details of the information requested.

If staff receive a subject access request they must immediately forward it to the DPO and notify the CEO or Principal.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at one of our primary schools may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our secondary school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification;
- May contact the individual via phone to confirm the request was made and/or clarify the request if required;
- Will respond without delay and within 1 month of receipt of the request;
- Will provide the information free of charge;
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual;
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests;
- Is contained in adoption or parental order records;
- Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

The Trust has an obligation to comply with the rights of individuals under the law. The Trust will comply with individual rights to:-

- Withdraw their consent to processing at any time;
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances);
- Prevent use of their personal data for direct marketing;
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests;
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement);
- Be notified of a data breach (in certain circumstances);
- Make a complaint to the ICO;
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Biometric recognition systems

In those Schools where we use pupils' biometric data as part of an automated biometric recognition system, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to not participate in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carers.

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

11. CCTV

We use CCTV in various locations on Trust premises to ensure its schools remain safe. We will adhere to the ICO's code of practice for the use of CCTV.

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

Any enquiries about the CCTV system should be directed to NET Central Team on 01933 627081, please also refer to the Trust CCTV policy.

12. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our schools and by the Trust.

In our primary schools:

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carers and pupil.

In our secondary school:

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.
Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carers and pupil. Where we do not need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns;
- Online on our school website or social media pages;
- Video footage or television recordings at local or national level.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Please see our Child Protection and Safeguarding policy or contact the relevant school for more information on our use of photographs and videos.

13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6);
- Completing data protection impact assessments (DPIA) where the Trust's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process);
- Integrating data protection into internal documents including this policy, any related policies and privacy notices;

- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance;
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant;
- Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply;
- Maintaining records of our processing activities, including:
- For the benefit of data subjects, making available the name and contact details of our Schools and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices);
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those how and why we are storing the data, retention periods and how we are keeping the data secure.

14. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use;
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access;
- Where personal information needs to be taken off site, staff must sign it in and out;
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals;
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices;
- Staff, pupils or Trustees/governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Acceptable Use Policy);
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Trust's

behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal data breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the Trust's data breach procedure.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a Trust context may include, but are not limited to:

- A non-anonymised dataset being published on the Trust or individual Schools websites which shows the exam results of pupils eligible for the pupil premium;
- Safeguarding information being made available to an unauthorised person;
- The theft of a school laptop containing non-encrypted personal data about pupils.

17. Training

All staff and Trustees/governors are provided with data protection training as part of their induction process and ongoing as required.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary.

19. Monitoring arrangements

The Trust and DPO are responsible for monitoring and reviewing this policy.

This policy will be reviewed **every 2 years** and shared with the Board of Trustees.

Links with other policies

This data protection policy is linked to our:

Child Protection and Safeguarding Policy

Acceptable Use Policy

CCTV policy

Biometric Policy

Appropriate Data Policy

Freedom of Information Policy

1. Introduction

Nene Education Trust (NET), along with all other Public Authorities, must comply with the Freedom of Information Act. The Act was created as an initiative to increase openness and transparency in Government, with the Freedom of Information Act passed on 30 November 2000.

The Act obliges organisations covered by it to publish certain information about their activities and, additionally, to make any other information (with a number of statutory exceptions) available upon request.

2. Scope

This policy is intended to cover all records created in the course of the business of NET. This includes email messages and other electronic records.

This policy applies to all NET employees, including temporary, casual or agency staff and contractors, consultants and suppliers working for, or on behalf of, NET.

3. What is a request under FOI

Any request for any information from the Trust is technically a request under the FOI, whether or not the individual making the request mentions the FOI. However, the ICO (Information Commissioner's Office) has stated that routine requests for information (such as a parent requesting a copy of a policy) can be dealt with outside of the provisions of the Act.

In all non-routine cases, if the request is simple and the information is to be released, then the individual who received the request can release the information, but must ensure that this is done within the timescale set out below. A copy of the request and response should then be sent to the Data Protection Officer.

All other requests should be referred in the first instance to the Data Protection Officer, who may allocate another individual to deal with the request. This must be done promptly, and in any event within three working days of receiving the request.

When considering a request under FOI, you must bear in mind that release under FOI is treated as release to the general public, and so once it has been released to an individual, anyone can then access it, and you cannot restrict access when releasing by marking the information "confidential" or "restricted".

4. Requesting information

The Freedom of Information Act 2000 provides public access to information held by public authorities. It does this in two ways:

- public authorities are obliged to publish certain information about their activities; and
- members of the public are entitled to request information from public authorities.

Under the second provision of the Act, the right to request information, anyone may make a request in writing for recorded information held by NET or its academies. A request for information not included already published must be made in writing to the Principal of each Academy or to the CEO of the Trust.

Upon receipt of a FOI request the individual receiving the request must promptly send a holding email to the requester acknowledging receipt of the request and setting out the timescale for receiving a response. See template wording for the holding email (appendix 1)

Requests for information will be met within 20 working days of receipt. Requests for information that require NET to complete a public interest test will be met within 40 working days of receipt. A working is a school day (one in which pupils are in attendance), subject to an absolute maximum of 60 normal working days (not school days) to respond.

5. Procedure for dealing with a request

When a request is received that cannot be dealt with by simply providing the information, it should be referred in the first instance to the Data Protection Officer, who may re-allocate to an individual with responsibility for the type of information requested.

The first stage in responding is to determine whether or not the Trust "holds" the information requested. The Trust will hold the information if it exists in computer or paper format. Some requests will require the Trust to take information from different sources and manipulate it in some way. Where this would take minimal effort, the Trust is considered to "hold" that information, but if the required manipulation would take a significant amount of time, the requestor should be contacted to explain that the information is not held in the manner requested, and offered the opportunity to refine their request. For example, if a request required the Trust to add up totals in a spread sheet and release the total figures, this would be information "held" by the Trust. If the Trust would have to go through a number of spread sheets and identify individual figures and provide a total, this is likely not to be information "held" by the Trust, depending on the time involved in extracting the information.

The second stage is to decide whether the information can be released, or whether one of the exemptions set out in the Act applies to the information. Common exemptions that might apply include:

Section 40 (1) – the request is for the applicant's personal data. This must be dealt with under the subject access regime in the DPA (Data Protection Act), detailed in paragraph 9 of the data protection policy above;

Section 40 (2) – compliance with the request would involve releasing third party personal data, and this would be in breach of the DPA principles as set out in the data protection policy;

Section 41 – information that has been sent to the Trust (but not the Trust's own information) which is confidential;

Section 21 – information that is already publicly available, even if payment of a fee is required to access that information;

Section 22 – information that the Trust intends to publish at a future date;

Section 43 – information that would prejudice the commercial interests of the Trust and / or a third party;

Section 38 – information that could prejudice the physical health, mental health or safety of an individual (this may apply particularly to safeguarding information);

Section 31 – information which may prejudice the effective detection and prevention of crime – such as the location of CCTV cameras;

Section 36 – information which, in the opinion of the chair of the board of trustees of the Trust, would prejudice the effective conduct of the Trust. There is a special form for this on the ICO's website to assist with the obtaining of the chair's opinion.

The sections mentioned in italics are qualified exemptions. This means that even if the exemption applies to the information, you also have to carry out a public interest weighting exercise, balancing the public interest in the information being released, as against the public interest in withholding the information.

6. Transferring requests for information

Should a request for information relate to North Northamptonshire Council, NET will acknowledge to the requester that the request relates to North Northamptonshire Council and refer the requester to North Northamptonshire Council, who will process this request for information, within 10 working days of receipt.

7. Subject access requests

Please refer to NET's Subject Access Request Procedure, or see page 8 in this policy on SARs.

8. Responding to a request

When responding to a request where the Trust has withheld some or all of the information the Trust must explain why the information has been withheld, quoting the appropriate section number and explaining how the information requested fits within that exemption. If the public interest test has been applied, this also needs to be explained. The letter should end by explaining to the requester how they can complain.

9. Exemptions

The Freedom of Information Act contains a number of exemptions whereby information can be withheld. NET may choose to withhold information if it falls within the scope of one or more of these exemptions. Where a request is made for information that includes exemptions, NET will apply a public interest test before deciding whether to disclose the information.

Where information is withheld under an exemption NET will, in most cases, inform the applicant as to why the information is being withheld, citing the exception.

10. Vexatious requests

The Act allows NET to refuse any requests that have the potential to cause a disproportionate or unjustified level of disruption, irritation or distress.

Decisions on whether a request is vexatious will be taken by the Chief Executive Officer with the assistance of legal advice where necessary.

11. Record keeping

All Freedom of Information requests will be logged and tracked by NET. This will aid identification of repeat, similar or vexatious requests.

12. Complaints

Applicants dissatisfied with NET's response to a request, including appeals against decisions to withhold information, may complain through NET's complaints procedure.

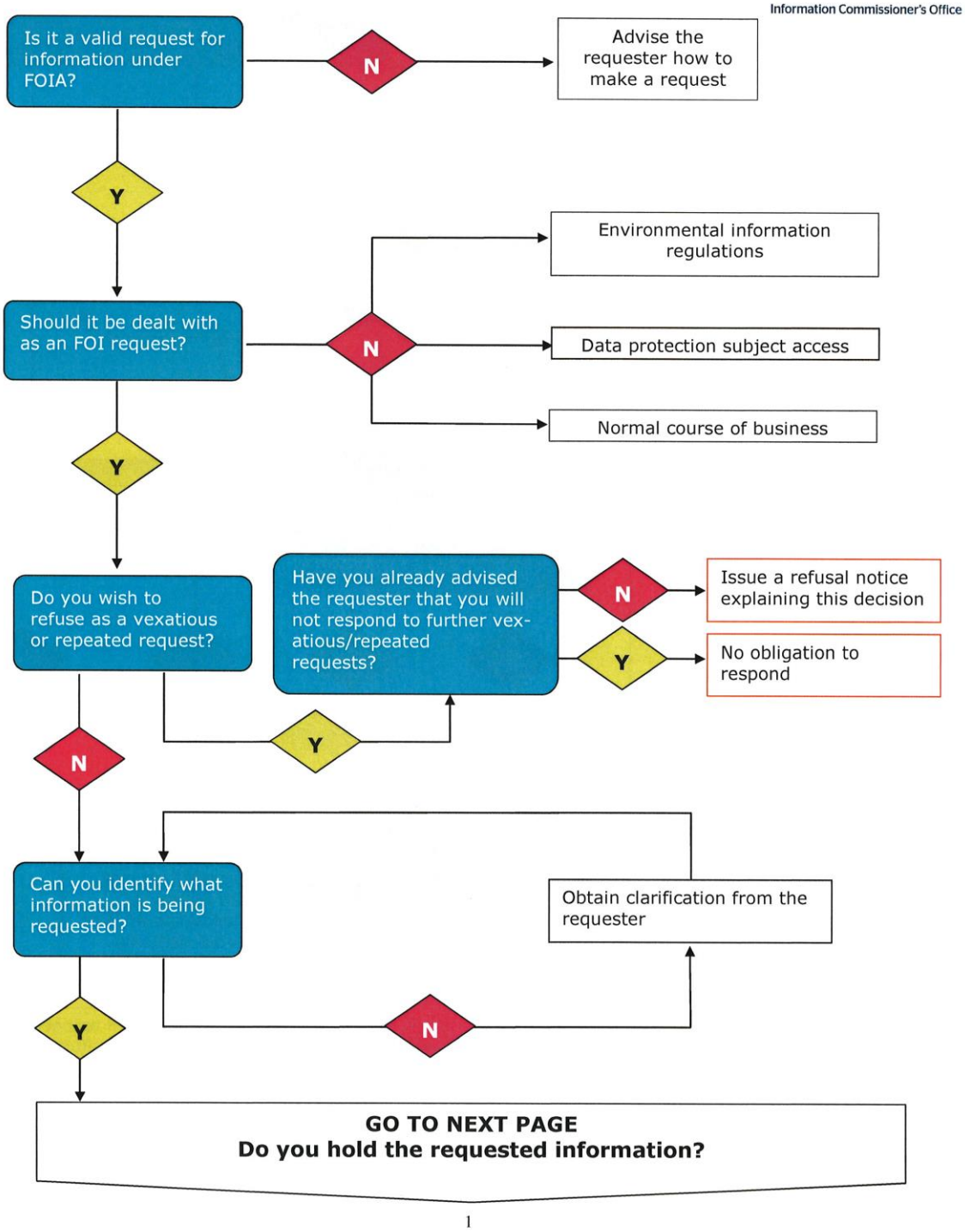
If, after exhausting NET's complaints procedure, you are still dissatisfied with the outcome, you may refer the matter to the Information Commissioner.

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Further information regarding the Freedom Information Act can be found direct from the ICO at the following link

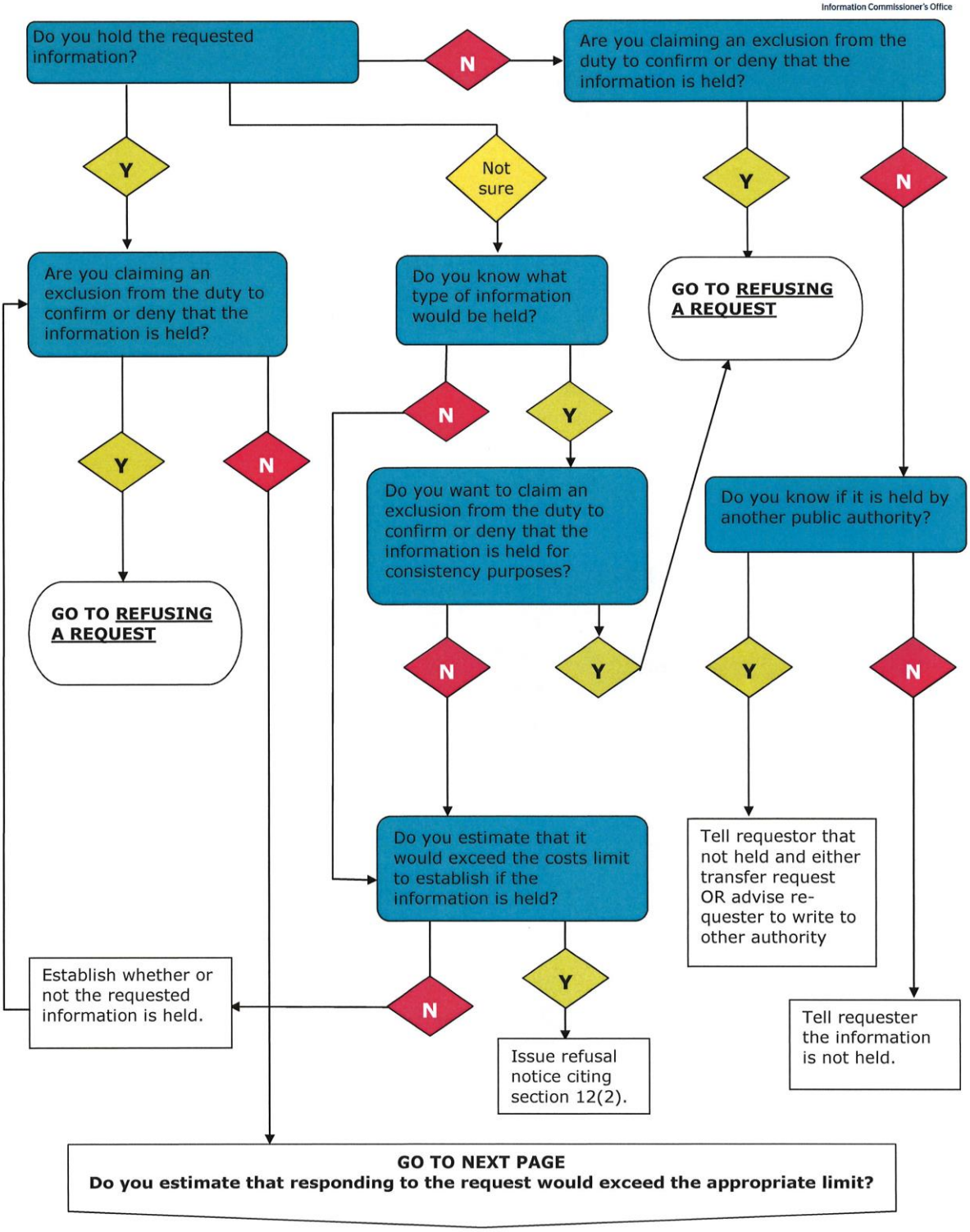
https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

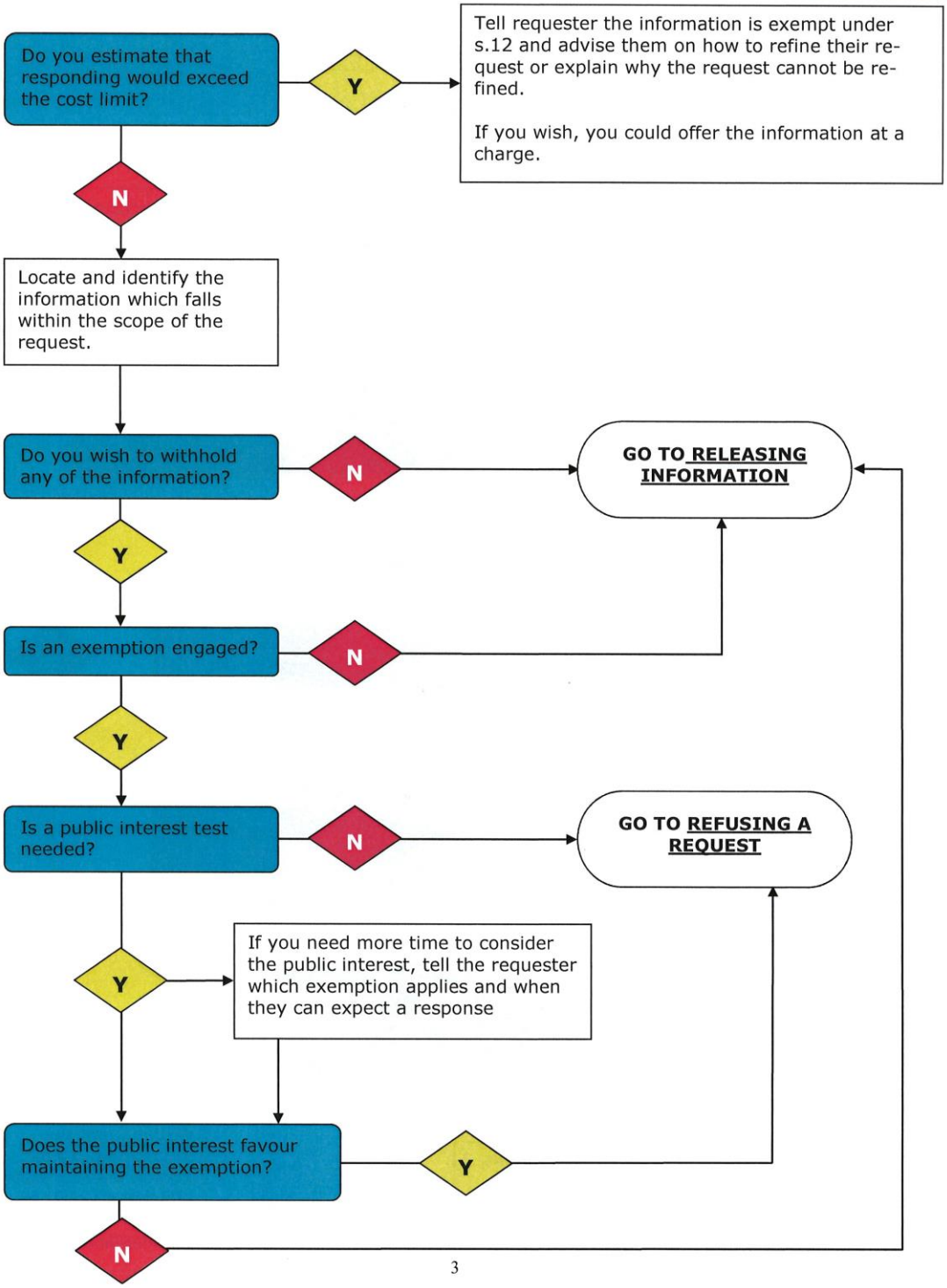
Start here



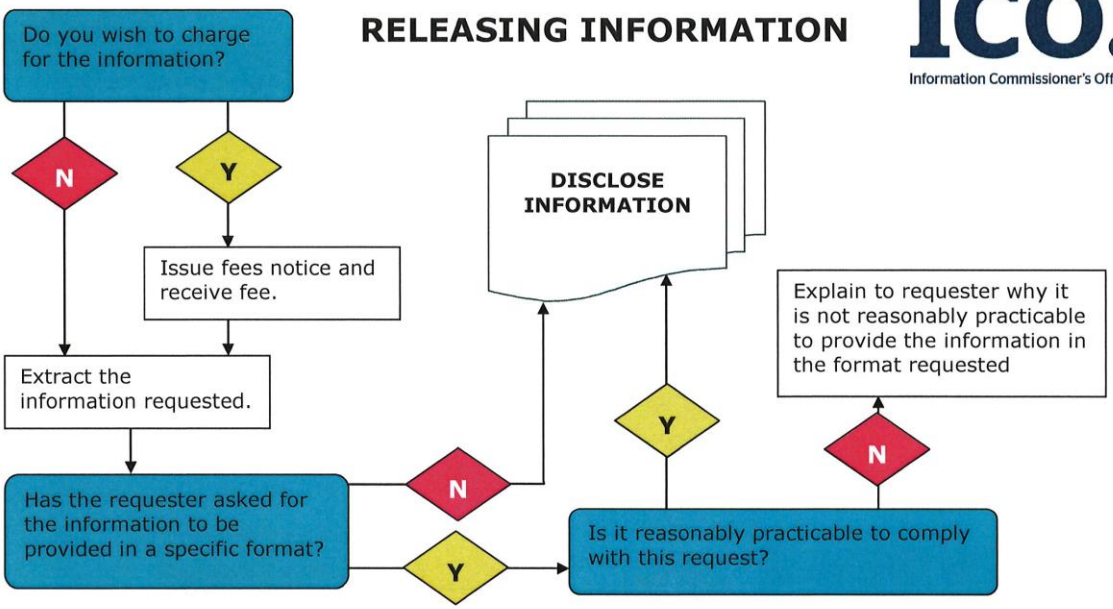
1

27 November 2012 v1.0

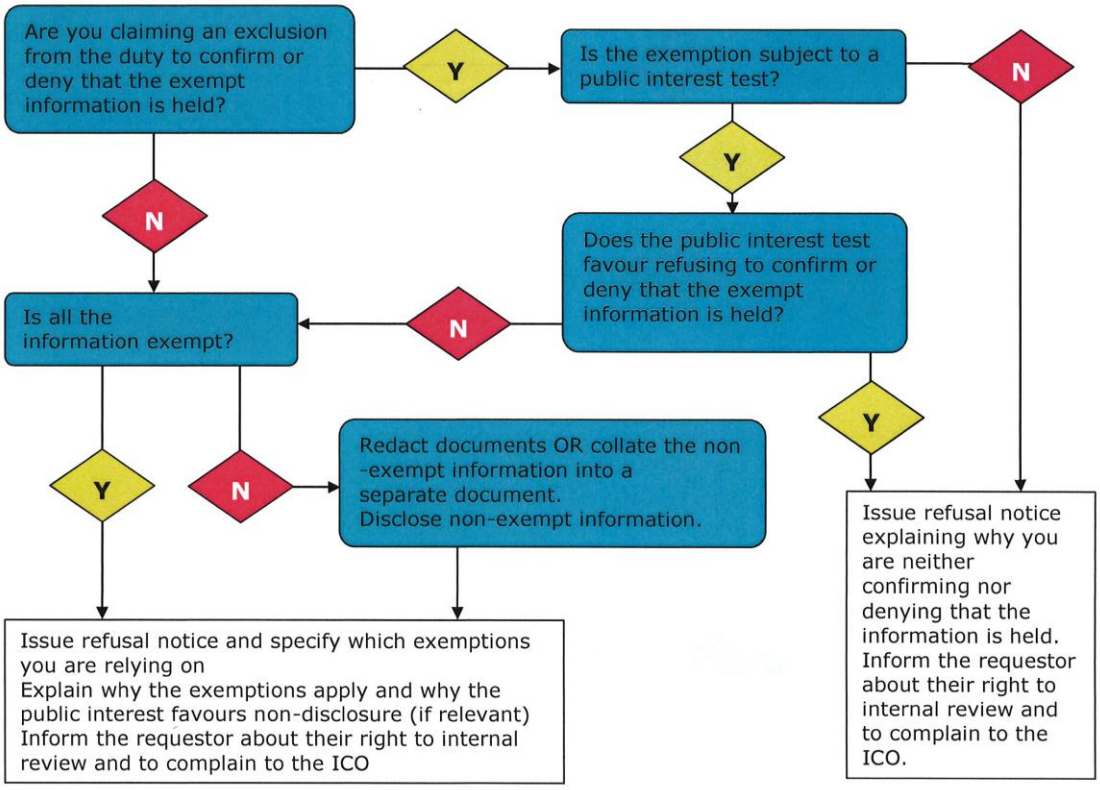

Do you hold the requested information?
N
Are you claiming an exclusion from the duty to confirm or deny that the information is held?
Y
Not sure
Y
N
Are you claiming an exclusion from the duty to confirm or deny that the information is held?
Do you know what type of information would be held?
GO TO REFUSING A REQUEST
N
Y
Y
N
Do you want to claim an exclusion from the duty to confirm or deny that the information is held for consistency purposes?
Do you know if it is held by another public authority?
GO TO REFUSING A REQUEST
N
Y
Y
N
Do you estimate that it would exceed the costs limit to establish if the information is held?
Tell requestor that not held and either transfer request OR advise requester to write to other authority
Establish whether or not the requested information is held.
N
Y
Issue refusal notice citing section 12(2).
Tell requester the information is not held.
GO TO NEXT PAGE
Do you estimate that responding to the request would exceed the appropriate limit?


Do you estimate that responding would exceed the cost limit?
Y
Tell requester the information is exempt under s.12 and advise them on how to refine their request or explain why the request cannot be refined.
If you wish, you could offer the information at a charge.
N
Locate and identify the information which falls within the scope of the request.
Do you wish to withhold any of the information?
N
GO TO RELEASING INFORMATION
Y
Is an exemption engaged?
N
Y
Is a public interest test needed?
N
GO TO REFUSING A REQUEST
Y
If you need more time to consider the public interest, tell the requester which exemption applies and when they can expect a response
Does the public interest favour maintaining the exemption?
Y
N

RELEASING INFORMATION



REFUSING A REQUEST



Appendix 1

Template holding email on receipt of a FOI

Dear xxxxxx

We acknowledge receipt of your FOI request received by email/letter dated xxxxxxx, we note the request relates to (set out here the subject of the FOI).

In line with the details contained in Nene Education Trust (NET) FOI policy section 2

Requests for information will be met within 20 working days of receipt. Requests for information that require NET to complete a public interest test will be met within 40 working days of receipt. A working is a school day (one in which pupils are in attendance), subject to an absolute maximum of 60 normal working days (not school days) to respond.

Yours sincerely