YARDLEY BAPTIST CHURCH

DATA PROTECTION POLICY

Policy author	**Steve Aylin**
Updated by	**Heather Kelcey**
Replaces	**Policy adopted at the church meeting May 2025**
Approved at Church Meeting	**July 2026**
Next Review Due	**July 2028 OR in case of significant changes to law, good practice guidelines or personnel**
Compliance monitoring	**Trustees**

Yardley Baptist Church is committed to protecting all information that we handle about people we support and work with, and to respecting people's rights around how their information is handled. This policy explains our responsibilities and how we will meet them.

Contents

Contents

Section A – What this policy is for 3

1. Policy statement 3
2. Why this policy is important 3
3. How this policy applies to you & what you need to know 3
4. Training and guidance 4

Section B – Our data protection responsibilities 4

5. What personal information do we process? 4
6. Making sure processing is fair and lawful 5
7. When we need consent to process data 7
8. Processing for specified purposes 7
9. Data will be adequate, relevant and not excessive 7
10. Accurate data 7
11. Keeping data and destroying it 7
12. Security of personal data 8
13. Keeping records of our data processing 8

Section C – Working with people we process data about (data subjects) 8

14. Data subjects' rights 8
15. Direct marketing 9

Section D – working with other organisations & transferring data 10

16. Sharing information with other organisations 10
17. Data processors 10
18. Transferring personal data outside the United Kingdom (UK) 10

Section E – Managing change & risks 10

19. Data protection impact assessments 10
20. Dealing with data protection breaches 11

Schedule 1 – Definitions and useful terms 12

[Schedule 2 – ICO Registration] 14

Appendix 1: Subject Access Requests 16

Section A – What this policy is for

1. Policy statement

1.1 YARDLEY BAPTIST CHURCH is committed to protecting personal data and respecting the rights of our **data subjects**; the people whose **personal data** we collect and use. We value the personal information entrusted to us and we respect that trust, by complying with all relevant laws, and adopting good practice.

We process personal data to help us:

a) maintain our list of church members and regular attenders
b) provide pastoral support for members and others connected with our church
c) provide services to the community
d) safeguard children, young people and adults at risk
e) recruit, support and manage staff and volunteers
f) maintain our accounts and records
g) promote our services
h) respond effectively to enquirers and handle any complaints.

1.2 This policy has been approved by the church's Charity Trustees (**YBC's data controller**) who are responsible for ensuring that we comply with all our legal obligations. It sets out the legal rules that apply whenever we obtain, store or use personal data.

2. Why this policy is important

2.1 We are committed to protecting personal data from being misused, getting into the wrong hands as a result of poor security or being shared carelessly, or being inaccurate, as we are aware that people can be upset or harmed if any of these things happen.

2.2 This policy sets out the measures we are committed to taking as an organisation and what each of us will do to ensure we comply with the relevant legislation.

2.3 In particular, we will make sure that all personal data is:

a) processed **lawfully, fairly and in a transparent manner**;
b) processed for **specified, explicit and legitimate purposes** and not in a manner that is incompatible with those purposes;
c) **adequate, relevant and limited to what is necessary** for the purposes for which it is being processed;
d) **accurate** and, where necessary, up to date;
e) **not kept longer than necessary** for the purposes for which it is being processed;
f) processed in a **secure** manner, by using appropriate technical and organisational means;
g) processed in keeping with the **rights of data subjects** regarding their personal data.

3. How this policy applies to you & what you need to know

3.1 **As an employee, trustee or volunteer** processing personal information on behalf of the church, you are required to comply with this policy. If you think that you have accidentally breached the policy it is important that you contact our Data Protection Trustee immediately so that we can take swift action to try and limit the impact of the breach.

Anyone who breaches the Data Protection Policy may be subject to disciplinary action, and where that individual has breached the policy intentionally, recklessly, or for personal benefit they may also be liable to prosecution or to regulatory action.

3.2 **As a leader/manager:** You are required to make sure that any procedures that involve personal data, that you are responsible for in your area, follow the rules set out in this Data Protection Policy.

3.3 **As a data subject of Yardley Baptist Church:** We will handle your personal information in line with this policy.

3.4 **As an appointed data processor/contractor:** Companies who are appointed by us as a data processor are required to comply with this policy under the contract with us. Any breach of the policy will be taken seriously and could lead to us taking contract enforcement action against the company or terminating the contract. Data processors have direct obligations under the GDPR, primarily to only process data on instructions from the controller (us) and to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved.

3.5 **Our Data Protection Trustee – the church secretary -** is responsible for advising Yardley Baptist Church and its staff and members about their legal obligations under data protection law, monitoring compliance with data protection law, dealing with data security breaches and with the development of this policy. Any questions about this policy or any concerns that the policy has not been followed should be referred to them at secretary@yardleybaptist.co.uk . The Data Protection Trustee remains at all times answerable to the YBC minister and trustees. Should anyone have any concerns about the actions of the Data Protection Trustee they should in the first instance communicate this to the minister.

3.6 Before you collect or handle any personal data as part of your work (paid or otherwise) for Yardley Baptist Church, it is important that you take the time to read this policy carefully and understand what is required of you, as well as the organisation's responsibilities when we process data.

3.7 Our procedures will be in line with the requirements of this policy, but if you are unsure about whether anything you plan to do, or are currently doing, might breach this policy you must first speak to the Data Protection Trustee

4. Training and guidance

4.1 We will provide general training for those who hold a leadership role to raise awareness of their obligations and our responsibilities, as well as to outline the law.

4.2 We may also issue procedures, guidance or instructions from time to time.

Section B – Our data protection responsibilities

5. What personal information do we process?

5.1 In the course of our work, we may collect and process information (personal data) about many different people (data subjects). This includes data we receive straight from the person it is about, for example, where they complete forms or contact us. We may also receive information about data subjects from other sources including, for example, previous employers and Due Diligence Checking Ltd.

5.2 We process personal data in both electronic and paper form and all this data is protected under data protection law. The personal data we process can include information such as names and contact details, education or employment details, dietary requirements and visual images of people.

5.3 In some cases, we hold types of information that are called **"special categories"** of data in the GDPR. This personal data can only be processed under strict conditions.

'Special categories' of data (as referred to in the GDPR) includes information about a person's: racial or ethnic origin; political opinions; religious or similar (e.g. philosophical) beliefs; trade union membership; health (including physical and mental health, and the provision of health care services); genetic data; biometric data; sexual life and sexual orientation.

5.4 We will not hold information relating to criminal proceedings or offences or allegations of offences unless there is a clear lawful basis to process this data such as where it fulfils one of the substantial public interest conditions in relation to the safeguarding of children and of individuals at risk or one of the additional conditions relating to criminal convictions set out in either Part 2 or Part 3 of Schedule 1 of the Data Protection Act 2018. This processing will only ever be carried out on the advice of the Ministries Team of the Baptist Union of Great Britain or our Regional Association Safeguarding contact person.

5.5 Other data may also be considered 'sensitive' such as bank details, but will not be subject to the same legal protection as the types of data listed above.

5.6 We record and broadcast our Sunday services, our church members' meetings and occasional other events via ZOOM. One of the 'special categories' of data about an individual is their religion and belief. With this in mind we are striving to ensure that we are always careful about our video recordings that often show members of our congregation.

The steps that we are taking :

- The sermons that we add to our website will be AUDIO ONLY - as from January 2024.
- We will work backwards through previous sermons to convert them from video to audio.
- The ZOOM link to our Sunday morning service will be regularly changed.
- The ZOOM RECORDING (which will still be VIDEO) will only be available for 12 months.
- All ZOOM links and recordings will continue to **ONLY** be sent to those on YBC CHURCHSUITE.
- Recipients will be asked to request permission from YBC's 'data protection trustee' – the church secretary, before sharing a ZOOM link with others.
- The framing of each service recording focussed on the activities at the front of church

- On each individual's CHURCHSUITE page there is a disclaimer that says :

  I give consent to my appearance in ZOOM recordings of YBC services.

  This has been set to '**YES**' by default - if you would like that to say '**NO**' then please contact the church secretary. You will also need to remain in the 'cafe section' of the church building during our Sunday morning services.

5.7 We also record data using our CCTV system – which is dealt with in our CCTV policy.

6. Making sure processing is fair and lawful

6.1 Processing of personal data will only be fair and lawful when the purpose for the processing meets a legal basis, as listed below, and when the processing is transparent. This means we will provide people with an explanation of how and why we process their personal data at the point we collect data from them, as well as when we collect data about them from other sources.

How can we legally use personal data?

6.2 Processing of personal data is only lawful if at least one of these legal conditions, as listed in Article 6 of the GDPR, is met:

a) the processing is **necessary for a contract** with the data subject;

b) the processing is **necessary for us to comply with a legal obligation**;

c) the processing is necessary to protect someone's life (this is called "**vital interests**");

d) the processing is necessary for us to perform a task in the **public interest**, and the task has a clear basis in law;

e) the processing is **necessary for legitimate interests** pursued by YARDLEY BAPTIST CHURCH or another organisation, unless these are overridden by the interests, rights and freedoms of the data subject.

f) If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their clear **consent**.

How can we legally use 'special categories' of data?

6.3 Processing of 'special categories' of personal data is only lawful when, in addition to the conditions above, one of the extra conditions, as listed in Article 9 of the GDPR, is met. These conditions include where:

a) the processing is necessary for **carrying out our obligations under employment and social security and social protection law**;

b) the processing is necessary for **safeguarding the vital interests** (in emergency, life or death situations) **of an individual** and the data subject is incapable of giving consent;

c) the processing is carried out in the **course of our legitimate activities** and only relates to our members or persons we are in regular contact with in connection with our purposes;

d) the processing is necessary for **pursuing legal claims**.

e) If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their **explicit consent**.

6.4 Before deciding which condition should be relied upon, we may refer to the original text of the GDPR as well as any relevant guidance, and seek legal advice as required.

What must we tell individuals before we use their data?

6.5 If personal data is collected directly from the individual, we will inform them [in writing] about; our identity/contact details and those of the Data Protection Trustee, the reasons for processing, and the legal bases, including explaining any automated decision making or profiling explaining our legitimate interests, and explaining, where relevant, the consequences of not providing data needed for a contract or statutory requirement; who we will share the data with; if we plan to send the data outside of the United Kingdom; how long the data will be stored and the data subjects' rights.

This information is commonly referred to as a 'Privacy Notice'.

This information will be given at the time when the personal data is collected.

6.6 If data is collected from another source, rather than directly from the data subject, we will provide the data subject with the information described in section 6.5 as well as: the categories of the data concerned; and the source of the data.

This information will be provided to the individual in writing and no later than within **1 month** after we receive the data, unless a legal exemption under the GDPR applies. If we use the data to communicate with the data subject, we will at the latest give them this information at the time of the first communication.

If we plan to pass the data onto someone else outside of YARDLEY BAPTIST CHURCH, we will give the data subject this information before we pass on the data.

7. When we need consent to process data

7.1 Where none of the other legal conditions apply to the processing, and we are required to get consent from the data subject, we will clearly set out what we are asking consent for,

including why we are collecting the data and how we plan to use it. Consent will be specific to each process we are requesting consent for and we will only ask for consent when the data subject has a real choice whether or not to provide us with their data.

7.2 Consent can however be withdrawn at any time and if withdrawn, the processing will stop. Data subjects will be informed of their right to withdraw consent and it will be as easy to withdraw consent as it is to give consent.

8. Processing for specified purposes

8.1 We will only process personal data for the specific purposes explained in our privacy notices (as described above in section 6.5.) or for other purposes specifically permitted by law. We will explain those other purposes to data subjects in the way described in section 6, unless there are lawful reasons for not doing so.

9. Data will be adequate, relevant and not excessive

9.1 We will only collect and use personal data that is needed for the specific purposes described above (which will normally be explained to the data subjects in privacy notices). We will not collect more than is needed to achieve those purposes. We will not collect any personal data “just in case” we want to process it later.

10. Accurate data

10.1 We will make sure that personal data held is accurate and, where appropriate, kept up to date. The accuracy of personal data will be checked at the point of collection and at appropriate points later on.

11. Keeping data and destroying it

11.1 We will not keep personal data longer than is necessary for the purposes that it was collected for.

12. Security of personal data

12.1 We will use appropriate measures to keep personal data secure at all points of the processing. Keeping data secure includes protecting it from unauthorised or unlawful processing, or from accidental loss, destruction or damage.

12.2 We will implement security measures which provide a level of security which is appropriate to the risks involved in the processing.

Measures will include technical and organisational security measures. In assessing what

measures are the most appropriate we will take into account the following, and anything else that is relevant:

a) the quality of the security measure;

b) the costs of implementation;

c) the nature, scope, context and purpose of processing;

d) the risk (of varying likelihood and severity) to the rights and freedoms of data subjects;

e) the risk which could result from a data breach.

12.3 Measures may include:

a) technical systems security;

b) measures to restrict or minimise access to data;

c) measures to ensure our systems and data remain available, or can be easily restored in the case of an incident;

d) physical security of information and of our premises;

e) organisational measures, including policies, procedures, training and audits;

f) regular testing and evaluating of the effectiveness of security measures.

13. Keeping records of our data processing

13.1 To show how we comply with the law we will keep clear records of our processing activities and of the decisions we make concerning personal data (setting out our reasons for those decisions).

Section C – Working with people we process data about (data subjects)

14. Data subjects' rights

14.1 We will process personal data in line with data subjects' rights, including their right to:

a) request access to any of their personal data held by us (known as a Subject Access Request); (See Appendix 1 for how we will respond to Subject Access Requests)

b) ask to have inaccurate personal data changed;

c) restrict processing, in certain circumstances;

d) object to processing, in certain circumstances, including preventing the use of their data for direct marketing;

e) data portability, which means to receive their data, or some of their data, in a format that can be easily used by another person (including the data subject themselves) or organisation;

f) not be subject to automated decisions, in certain circumstances; and

g) withdraw consent when we are relying on consent to process their data.

14.2 If a trustee receives any request from a data subject that relates or could relate to their data protection rights, this will be forwarded to our Data Protection Trustee **immediately**.

14.3 We will act on all valid requests as soon as possible, and at the latest within **one calendar month**, unless we have reason to, and can lawfully extend the timescale. This can be extended by up to two months in some circumstances.

14.4 All data subjects' rights are provided free of charge.

14.5 Any information provided to data subjects will be concise and transparent, using clear and plain language.

15. Direct marketing

15.1 We will comply with the rules set out in the GDPR, the Privacy and Electronic Communications Regulations (PECR) and any laws which may amend or replace the regulations around **direct marketing**. This includes, but is not limited to, when we make contact with data subjects by post, email, text message, social media messaging, telephone (both live and recorded calls) and fax.

Direct marketing means the communication (by any means) of any advertising or marketing material which is directed, or addressed, to individuals. "Marketing" does not need to be selling anything, or be advertising a commercial product. It includes contact made by organisations to individuals for the purposes of promoting the organisation's aims.

15.2 Any direct marketing material that we send will identify YARDLEY BAPTIST CHURCH as the sender and will describe how people can object to receiving similar communications in the future. If a data subject exercises their right to object to direct marketing we will stop the direct marketing as soon as possible.

Section D – working with other organisations & transferring data

16. Sharing information with other organisations

16.1 We will only share personal data with other organisations or people when we have a legal basis to do so and if we have informed the data subject about the possibility of the data being shared (in a privacy notice), unless legal exemptions apply to informing data subjects

about the sharing. Only authorised and properly instructed [staff/Trustees] are allowed to share personal data.

16.2 We will keep records of information shared with a third party, which will include recording any exemptions which have been applied, and why they have been applied. We will follow the ICO's statutory ***Data Sharing Code of Practice*** (or any replacement code of practice) when sharing personal data with other data controllers. Legal advice will be sought as required.

17. Data processors

17.1 Before appointing a contractor who will process personal data on our behalf (a data processor) we will carry out due diligence checks. The checks are to make sure the processor will use appropriate technical and organisational measures to ensure the processing will comply with data protection law, including keeping the data secure, and upholding the rights of data subjects. We will only appoint data processors who can provide us with sufficient guarantees that they will do this.

17.2 We will only appoint data processors on the basis of a written contract that will require the processor to comply with all relevant legal requirements. We will continue to monitor the data processing, and compliance with the contract, throughout the duration of the contract.

17.3 Current Data processors may include providers of church management systems, website hosting services, cloud-based communication platforms (including Zoom), email services and other technology suppliers. Appropriate due diligence will be undertaken before such providers are appointed.

18. Transferring personal data outside the United Kingdom (UK)

18.1 Personal data cannot be transferred (or stored) outside of the United Kingdom unless this is permitted by the UK GDPR. This includes storage on a "cloud" based service where the servers are located outside the UK.

18.2 Some of the third-party services used by Yardley Baptist Church, including providers of website hosting, email, cloud storage, online meetings and communications, may process or store personal data outside the United Kingdom, however, we will only transfer data outside the UK where it is permitted by one of the conditions for non-UK transfers in the UK GDPR. These conditions include:

- transfers to countries recognised by the UK Government as providing an adequate level of protection;
- the use of International Data Transfer Agreements (IDTAs), Addendums to Standard Contractual Clauses, or other approved transfer mechanisms;
- reliance on other lawful transfer provisions permitted under UK GDPR where appropriate.

18.3 Before appointing a supplier that may process personal data outside the UK, we will consider whether the supplier provides appropriate technical, organisational and contractual protections for personal data.

Section E – Managing change & risks

19. Data protection impact assessments

19.1 When we are planning to carry out any data processing which is likely to result in a high risk we will carry out a Data Protection Impact Assessment (DPIA). These include situations when we process data relating to vulnerable people, trawling of data from public profiles, using new technology, and transferring data outside the UK. Any decision not to conduct a DPIA will be recorded.

19.2 We may also conduct a DPIA in other cases when we consider it appropriate to do so. If we are unable to mitigate the identified risks such that a high risk remains we will consult with the ICO.

19.3 DPIAs will be conducted in accordance with the ICO's Code of Practice 'Conducting privacy impact assessments'.

20. Dealing with data protection breaches

20.1 Where staff or volunteers, [or contractors working for us], think that this policy has not been followed, or data might have been breached or lost, this will be reported **immediately** to the Data Protection Trustee.

20.2 We will keep records of personal data breaches, even if we do not report them to the ICO.

20.3 We will report all data breaches which are likely to result in a risk to any person, to the ICO. Reports will be made to the ICO within **72 hours** from when someone in the church becomes aware of the breach.

20.4 In situations where a personal data breach causes a high risk to any person, we will (as well as reporting the breach to the ICO), inform data subjects whose information is affected, without undue delay.

This can include situations where, for example, bank account details are lost or an email containing sensitive information is sent to the wrong recipient. Informing data subjects can enable them to take steps to protect themselves and/or to exercise their rights.

Schedule 1 – Definitions and useful terms

The following terms are used throughout this policy and have their legal meaning as set out within the GDPR. The GDPR definitions are further explained below:

Data controller means any person, company, authority or other body who (or which) determines the means for processing personal data and the purposes for which it is processed. It does not matter if the decisions are made alone or jointly with others.

The data controller is responsible for the personal data which is processed and the way in which it is processed. We are the data controller of data which we process.

Data processors include any individuals or organisations, which process personal data on our behalf and on our instructions e.g. an external organisation which provides secure waste disposal for us. This definition will include the data processors' own staff (note that staff of data processors may also be data subjects).

Data subjects include all living individuals who we hold or otherwise process personal data about. A data subject does not need to be a UK national or resident. All data subjects have legal rights in relation to their personal information. Data subjects that we are likely to hold personal data about include:

- the people we care for and support;
- our office holders, employees (and former employees);
- consultants/individuals who are our contractors or employees
- volunteers;
- tenants;
- trustees;
- complainants;
- supporters;
- enquirers;
- friends and family;
- advisers and representatives of other organisations

ICO means the Information Commissioners Office which is the UK's regulatory body responsible for ensuring that we comply with our legal data protection duties. The ICO produces guidance on how to implement data protection law and can take regulatory action where a breach occurs.

Personal data means any information relating to a natural person (living person) who is either identified or is identifiable. A natural person must be an individual and cannot be a company or a public body. Representatives of companies or public bodies would, however, be natural persons.

Personal data is limited to information about living individuals and does not cover deceased people.

Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Privacy notice means the information given to data subjects which explains how we process their data and for what purposes.

Processing is very widely defined and includes any activity that involves the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing can also include transferring personal data to third parties, listening to a recorded message (e.g. on voicemail) or viewing personal data on a screen or in a paper document which forms part of a structured filing system. Viewing of clear, moving or stills images of living individuals is also a processing activity.

Special categories of data includes information about a person's:

- Racial or ethnic origin
- Political opinions
- Religious or similar (e.g. philosophical) beliefs
- Trade union membership
- Health (inc physical and mental health, and the provision of health care services)
- Genetic data
- Biometric data
- Sexual life and sexual orientation

[Schedule 2 – ICO Registration]

Data Controller: Yardley Baptist Church

Registration Number: ZA379087

Date Registered: 19 May 2019

Registration updated annually on (or near) 18th May

Appendix 1: Subject Access Requests

a) Any person is entitled to ask to for a copy of the data which YBC holds about them. This is called a Subject Access Request, or SAR for short.
b) Requests can be made verbally or in writing: they do not have to be in writing or use specific phrases or quote any particular legislation.
c) Subject Access Requests should be made to the YBC Data Protection Officer, who is the Church Secretary. If a SAR is made to any other leader or volunteer at YBC, the request must be forwarded to the Church Secretary straight away. The Data Protection Officer will take the lead on complying with the SAR, unless they are unable, for example because of illness or holiday, in which case another member of the church leadership will be designated to take the lead in complying with the request.
d) Once YBC receives a SAR, we have one calendar month to provide the information requested. However, if the request is complex, we can extend the time limit by a further 2 months
e) Subject access requests are provided free of charge, unless the request is manifestly unfounded or excessive, or if an individual requests further copies of their data. If a fee is charged, we do not need to comply with the request until we have received the fee. However, we should request the fee promptly and at the latest within one month of receiving the SAR.
f) If a child makes a SAR, we should consider whether the child is mature enough to understand their rights. If the request is from a child and we are confident they can understand their rights, we should usually respond directly to the child. We may, however, allow the parent or guardian to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child. If a child is competent, they may authorise someone else, other than a parent or guardian, to make a SAR on their behalf.

On receiving a Subject Access Request

1) The Data Protection Officer, or in their absence another member of the church leadership, will confirm that the request is a SAR, and will log it as such, noting the date on which the request was first received, and the date by which a response must be given. See Appendix 2 for SAR record log template.

2) The DPO or other appointed leader will acknowledge the request and if necessary will verify the identity of the person making the request (see Appendix 2). If necessary, they will clarify what data is required, for example, data which relates to a specific issue, is for a specific timeframe or held in a specific way. The date by which the SAR will be actioned will be notified to the requester.

3) The DPO or other appointed leader will then make reasonable efforts to find and retrieve the requested information. We do **not** have to disclose everything we hold which relates to the data subject. There are some exceptions, such as confidential references and documents which also relate to another person (third party data). The BUGB Data Protection Team can be contacted for advice on this.

4) Any third party information must be redacted before providing the information. This must be done in such a way as to make the redacted information irretrievable. **It is not sufficient to highlight or blackout text in Microsoft Word, and to then save the document as a PDF**. Sometimes it may be easier to lift the requester's personal data out of a document into a separate document that can be disclosed.

5) The requested information will be sent to the requester as promptly as possible, but within the agreed time frame as documented in the log (Appendix 2).

References

Data Protection Guidance: Data Subject Access Requests (DSARs) February 2026
https://www.baptist.org.uk/Publisher/File.aspx?id=230931 (accessed 2/7/26)

ICO A guide to subject Access
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/subject-access-requests/a-guide-to-subject-access (accessed 2/7/26)

Appendix 2: Subject access Request log

Date request received	
Request made by	
Request made to	
Designated member of leadership who will lead in fulfilling the SAR	
Requester's Identification verified by: (eg, passport, driving license, utility bill or bank statement)	
Is the Requester A requesting their own information, or B requesting information on behalf of someone else?	
If B: Authorisation to request information on behalf of another individual (eg signed authorisation letter from data subject; original or certified copy of power of attourney)	
Response due by (usually one month after receipt of request)	
If an extension to the response due date is applied:	
Response due by (with up to 2 month extension applied, if applicable)	
Reason for application of due date extension	
Date response provided by	