



SIR ROBERT PATTINSON ACADEMY

ACADEMY PRIVACY POLICY

Date Reviewed in School: January 2026

Date Approved by Trustees: 9 February 2026

Date to be Reviewed: January 2027

PRIVACY NOTICE

HOW WE USE YOUR DATA

DATA CONTROLLER

We are Sir Robert Pattinson Academy. Our Academy is located at Moor Lane, North Hykeham, Lincoln LN6 9AF. In this privacy notice, we refer to ourselves as **the Academy**, or 'we' and 'us' etc.

The Academy is a 'controller' of data. This means that, under the UK General Data Protection Regulation (**GDPR**) and the Data Protection Act 2018 (**DPA**), we may control and process your personal data in connection with any personal information collected or received by us.

APPLICATION OF THIS NOTICE

This notice applies to anyone who is affected by the education we provide, including:

- Staff
- Pupils
- Parents/Carers
- Contractors and suppliers
- Job applicants
- Visitors

INTRODUCTION

The GDPR and the DPA govern the controlling and processing (or the use or holding) of personal data. Personal data is essentially any information about specific identifiable living individuals. The GDPR and the DPA also give those individuals certain rights in respect of their information. These rights are described below under the heading 'Your Rights'.

The purpose of this notice is to supply you with the required information at the time of providing us with your personal data. This notice sets out the essentials in relation to personal information collected by the Academy, and aims to help your confidence regarding the privacy and the security of your personal information.

PLEASE READ THIS PRIVACY NOTICE CAREFULLY. BY VISITING OUR WEBSITE OR PROVIDING US WITH YOUR PERSONAL INFORMATION, YOU INDICATE YOUR AGREEMENT TO OUR USE OF YOUR PERSONAL INFORMATION AS SET OUT IN THIS PRIVACY NOTICE.

CHANGES TO THIS NOTICE

We reserve the right to make changes to this notice (and our policy on data protection) at any time and we may notify you of changes to this notice by posting an updated version of this notice on our

website. You should check this page occasionally to ensure you are happy with any changes to this notice.

KEEPING US INFORMED

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

PERSONAL DATA WE MAY COLLECT ABOUT YOU

Personal information means any information about you from which you can be identified, but it does not include information where your identity has been removed ('**anonymous data**').

As the 'controller' of personal information, we are responsible for how that data is managed. The GDPR and the DPA set out our obligations to you and your rights in respect of how we manage your personal information.

As the 'controller' of your personal information, we will ensure that the personal information we hold about you is:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

Information collected by us:

We may collect, use, store and transfer information about you in several different ways and this information may be classified in different categories. Please take care when submitting information to us. Only provide us with information that you are happy for us to process in accordance with this notice, particularly with regard to confidential or sensitive information.

In the course of providing our services, or when processing any application you make to us, or in employing or engaging you, the following types of data may be collected from you:

Contact and Identification Data: includes your name, address and contact details (including email address and telephone number), gender and or pronoun preferences (for the purposes of addressing you correctly). For pupils, this also includes your pupil number.

Pupil Data: includes information about you as a pupil, applicant or former pupil of our Academy,

including your date of birth, school year, attendance information, next of kin and family information (including their contact, address and status details), disciplinary and school record, examination scripts and marks, references given by other schools, correspondence about pupils with parents, pupil interest and extra curriculum activities, consent forms, images of pupils and images captured on CCTV

Special Category Pupil Data: includes special categories of information including nationality, racial or ethnic origin, language information, dietary needs, religious or cultural information, information about any disability or special educational needs, age, criminal record, safeguarding referrals and other information

Pupil Biometric Data: Pupil fingerprint information (to be used as part of our automated biometric recognition system)

Technical Data includes internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this website; this also include information about your location.

Payment Information: this includes your bank and credit card details.

DBS Information: includes information about criminal convictions, including convictions which may be regarded by law as 'spent'; please note that this information is a form of special category of information for the purposes of the GDPR.

CCTV Data: information, including both still and moving images, obtained from our CCTV system.

SOURCES OF PERSONAL INFORMATION

We collect personal information from a variety of sources. This includes:

- When pupils join our Academy, either at Year 7 or some other time as part of the admission process
- When people interact with our staff, either face-to-face or by telephone
- When communicating with the Academy, or its staff, in writing through email or letter
- We may be provided with information about a pupil from other schools, safeguarding officers, law enforcement or the local authority
- We capture images of individuals within our grounds via our CCTV system
- From government bodies such as the Department of Education or Ofsted
- If you are a pupil over the age of 14 when you enrol with us, the Learning Records Service will also give us the unique learner number (ULN) and may also give us details about your qualifications
- If you are a job candidate, or member of staff, or trustee, we may collect information about you from previous employers and information that is available publicly, such as through social media

REASONS WE COLLECT AND USE YOUR PERSONAL INFORMATION

When we process your personal information, for whatever reason, we rely on one or more of the following grounds within the GDPR, depending on the reason why we are processing the information:

- Article 6(1)(a) – processing is conducted with your **consent** to process personal data for specified purposes (**Consent**)
- Article 6(1)(c) – processing is necessary for us to protect your **vital interests**, or the vital interest of someone else (**Vital Interest**)
- Article 6(1)(d) – processing is necessary for us to demonstrate compliance with our **regulatory framework** and the law (**Compliance**)
- Article 6(1)(f) – to process your personal data in pursuit of **legitimate interests** (**Legitimate Interests**)

We will only use your personal data to the extent permitted by the law. The Academy needs to process data for a variety of reasons, including as part of its duty to provide education. In general, the reasons why we might process your personal information are as follows:

Reason for Using Data	Type of Data	Legal Basis
To provide education to our pupils, including testing and assessing them and to support pupil learning	Contact and Identification; Pupil; Special Category Pupil	Compliance; legitimate interests
To meet or assess special educational needs	Contact and Identification; Pupil; Special Category Pupil	Compliance
To foster and maintain our relationships with alumni and the local community	Contact and Identification	Legitimate interests
To communicate with pupils and parents/carers	Contact and Identification; Pupil; Special Category Pupil	Compliance; legitimate interests
To process purchases from our Academy shop	Contact and Identification; Payment	Legitimate interests
To process purchases from our Academy canteen	Contact and Identification; Payment; Biometric	Consent; legitimate interests
To confirm the identify of prospective pupils and process and determine applications for admissions	Contact and Identification; Pupil; Technical	Compliance; legitimate interests
To enable relevant authorities such as Ofsted to monitor the Academy's performance and to intervene or assist with incidents as appropriate	Contact and Identification; Pupil; Special Category Pupil	Compliance

To give and receive information and references about past, current and prospective staff and pupils	Contact and Identification; Pupil; Special Category Pupil; DBS	Legitimate interests
To safeguard pupils' welfare and provide appropriate pastoral care	Contact and Identification; Pupil; Special Category Pupil	Compliance; legitimate interests; vital interests
To monitor, as appropriate, use of the Academy's IT and communications systems in accordance with the Academy's IT acceptable use policy	Technical	Compliance; legitimate interests
To monitor compliance with and enforce the rules of our behaviour policy	Contact and Identification; CCTV; Pupil; Technical	Compliance; legitimate interests
For marketing and promotional purposes and for keeping the community up-to-date with our campaigns, appeals, work and successes	Contact and Identification; Technical	Consent
For the purposes of detecting and preventing crime, including crime within our Academy such as damage to property and for the safety of our staff and pupils	Contact and Identification; Pupil; CCTV	Compliance; legitimate interests
To carry out or cooperate with any external complaints, disciplinary or investigation process	All data	Compliance; legitimate interests
To take appropriate action in the event of an emergency, incident or accident, including the disclosure of an individual's medical condition or other relevant information where it is in the individual's interests to do so: for example, for medical advice, for social protection, safeguarding, and cooperation with police or social services, for insurance purposes or to caterers or organisers of academy trips who need to be made aware of dietary or medical needs	Contact and Identification; Pupil; Special category pupil	Vital interests
To comply with our legal obligations to provide people with parental responsibility information about pupil progress and attainment	Contact and Identification; Pupil	Compliance
To use data analytics to improve and enhance our operations	Technical	Legitimate Interests

WHO HAS ACCESS TO YOUR PERSONAL INFORMATION?

Under no circumstances do we sell, lease or monetise your personal information. We share information with third parties, but only where we have a legal right or responsibility to do so.

Generally speaking, information that is shared within the Academy as part of our duty to provide education is done so on a “need-to-know basis”, with particular care being taken in respect of special categories of data, such as medical and SEN information. Where we supply personal information to third parties, we encourage people to look at the Privacy Policies in respect of each third party if they want to know more about how their data is used and looked after. Privacy Policies are usually found on the homepage of a supplier’s website.

We have set out below the details of third parties with whom we share data and why:

Local Authority Designated Officer: Information may be shared where we are obliged to make a safeguarding referral. This information is handled by the local authority in accordance with their own policies. In the case of the Academy, the local authority is Lincolnshire County Council.

Other safeguarding authorities: this may include social services and child protection services, and the police

Parents: As a general rule, we share information about pupils with parents and other individuals with parental responsibility. If a pupil asks us not to provide information to a parent, or person with parental responsibility, and they understand the nature and legal consequences of their request, then we will usually honour this, unless the law requires us not to.

Examining Bodies: As part of statutory examinations, it is necessary for us to provide pupil information to examining bodies, including names and other personal information as well as tests and papers.

Health and social welfare organisations: In order to support the health, well-being, and safety of our students, we may share relevant personal information with health and social care agencies. Such sharing is crucial for delivering health services and support, including vaccinations, mental health support, and safeguarding against abuse or neglect. It also enables these agencies to carry out their statutory responsibilities effectively.

Department of Education: As part of our public interest obligation, we are required to provide specific sets of data to the Department for Education (DfE) on a regular basis. This includes information related to school enrolment, attendance, academic progress, and pupil characteristics. The DfE uses this data to meet its statutory responsibilities, such as monitoring educational progress and policy development, and to enable the production of national educational statistics. We ensure that the data shared is limited to what is necessary and relevant for the DfE's lawful purposes. For more information on how the DfE processes this data, please refer to [DfE's privacy notice](#).

The Uniform Shop: This is our designated uniform supplier. To facilitate the purchase and distribution of school uniforms, we may share limited personal information with them. This information typically includes student names, year groups, and sizes to ensure the correct fitting and allocation of uniforms.

Sparx Learning: To enhance the educational experience and provide personalized learning opportunities, we collaborate with Sparx Learning, an educational technology provider. In this partnership, we may share limited student data such as names, year groups, and academic performance data.

This information is used by Sparx Learning to tailor their educational tools and resources to the specific needs of our students, facilitating a more effective and engaging learning process. We recommend that parents and guardians review Sparx Learning's Privacy Policy to understand their data handling practices.

Applicaa and other information processing software: To assist us with school administration, we use Applicaa, a provider of school management software solutions. We also use SIMS (School Information Management System) and Frog Drive. These platforms are all software that help us to manage and administer information about our school community. As part of this, we may share certain student and parent information with these various providers. This can include student names, contact details, academic records, and attendance data. Applicaa uses this information to facilitate various school management functions such as admissions processing, attendance tracking, and academic reporting. To fully understand how our providers manage and protect personal data, we encourage parents, guardians, and students to review the providers' Privacy Policies.

Our website and ICT providers: to enable us and them to deliver their service to us, carry out analysis and research on demographics, interests and behaviour of our users and supporters to help us gain a better understanding of them to enable us to improve our services. This may include connecting data we receive from you on the website to data available from other sources. Your personally identifiable data will only be used where it is necessary for the analysis required, and where your interests for privacy are not deemed to outweigh their legitimate interests in developing new services for us.

Other bodies and entities that we may share personal information with are as follows:

- **Lincolnshire County Council**, For purposes such as monitoring educational progress and providing support services
- Other relevant local education authorities where, for example, we are taking a pupil from a different area of the country and it is necessary to liaise with the in their area
- **Ofsted**, for inspection and regulatory purposes
- **Universities** and other education providers, for applications or transfers, or for collaborative educational programs
- **School transport** providers, for arranging and managing school transport services
- Our **contractors**, and **professional advisers**, including our **auditors**
- **HMRC**, as part of our legal obligations in respect of staff remuneration
- Our **HR advisers** and **IT consultants**;
- **Governors**
- **Police** and law enforcement agencies
- Payment service providers such as **Stripe** (when you use our school shop)
- **Cloud storage services**, although always within the EEA. We currently use **Veeam**.
- **System security tools**, such as firewalls and Impero: sometimes these systems require access to internet use history, but logs are encrypted and destroyed after a certain period of time.

THE NATIONAL PUPIL DATABASE (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department.

It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law to provide information about our pupils to the Department of Education as part of statutory data collections such as the school census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013. To find out more about the NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- Conducting research or analysis
- Producing statistics
- Providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether the Department releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- Who is requesting the data
- The purpose for which it is required
- The level and sensitivity of data requested: and
- The arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>.

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: <https://www.gov.uk/government/publications/national-pupil-database-requests-received>.

To contact the Department of Education: <https://www.gov.uk/contact-dfe>.

THIRD PARTY LIABILITY

We are not liable for the actions and inactions of third parties. In particular, you agree that when third parties are the controller of data (such as the DfE or LAE), then they are responsible for keeping your data safe once you have provided data to them. We have no control or responsibility over this.

Our website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you.

We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

KEEPING YOUR DATA SECURE

Whilst we cannot guarantee that unauthorised access to your data will never occur, we will use reasonable technical and organisational measures to safeguard your personal data, for example:

- Access to our systems is controlled by password and username which are unique to the user;
- We store your electronic personal data on secure servers;
- We store your paper records in locked fire-proof storage rooms;
- Payment details are encrypted;
- We always limit access to data about you (for example, data is shared with staff on a need-to-know basis only);
- We vet third party suppliers where they supply services to us that might involve processing your data to ensure that they also have proper technical and organisational measures to safeguard your personal data;
- Where necessary, we enter into professionally drafted data sharing and data processing agreements with third parties that focus on safeguarding personal data and comply with the GDPR;
- We take advice from experts on the GDPR and the DPA where we need it;
- We train our staff in data protection and awareness and we have policies and procedures in place for dealing with the unlikely event of data breaches

Our commitment to data security involves a continuous process of improvement. We are dedicated to regularly updating our security practices in line with technological advancements and legal requirements to ensure the ongoing confidentiality, integrity, and availability of personal data. However, we advise you to take great care over your personal data. Do not provide personal information about yourself or anybody else unless you are satisfied you are taking proper precautions first.

Non-sensitive details (your contact details and preferences for example) are transmitted normally over the Internet, and this can never be guaranteed to be 100% secure. As a result, while we strive to protect your personal information, we cannot guarantee the security of any information you transmit to us, and you do so at your own risk.

TRANSFERRING YOUR INFORMATION OUTSIDE OF EUROPE

We do not, as a matter of course, transfer personal information outside of the European Economic Area (**EEA**).

However, in the course of our educational and administrative operations, we utilise Microsoft-based cloud storage solutions for storing and processing personal data. Microsoft's cloud services, including Azure and Office 365, may involve the transfer of personal data to data centers located outside of the EEA.

We ensure that any transfer of personal data outside the EEA using Microsoft's services is carried out in compliance with the UK GDPR. Microsoft adheres to robust data protection standards and commitments, including:

1. **Data Protection Measures:** Microsoft implements strong data security measures to protect data from unauthorised access and breaches.
2. **Standard Contractual Clauses (SCCs):** Microsoft incorporates Standard Contractual Clauses in its contracts, which are approved mechanisms to ensure that any personal data leaving the EEA will be transferred in compliance with EU data protection law.
3. **EU-U.S. Privacy Shield Framework:** Although the EU-U.S. Privacy Shield Framework has been invalidated, Microsoft continues to adhere to its principles and has committed to additional safeguards for data transfers.
4. **Data Localization Options:** Where possible, we opt for data storage within the UK or EEA to minimise data transfer risks.

We regularly review our data storage and processing practices to ensure they align with legal requirements and best practices for data protection. For more detailed information on how Microsoft processes and protects personal data, we recommend reviewing Microsoft's Privacy Statement, available on their website.

HOW LONG DO WE KEEP YOUR DATA FOR?

We are committed to only retaining personal data for as long as necessary for the purposes for which it was collected, in accordance with our legal obligations and best practice guidelines. The length of time for which we retain data varies depending on the nature of the information and the reasons for which it is processed.

1. **Pupil Data:** Personal data relating to pupils, including academic, health, and welfare records, is typically retained until the pupil reaches the age of 25 or for a period of 6 years after they cease to be a pupil at the academy, whichever is longer. This is in line with the Department for Education's (DfE) guidelines.

2. **Staff Data:** Personal data of staff members is held for the duration of their employment and thereafter for a period consistent with employment law and best practice, usually no longer than 6 years after the end of employment.
3. **Financial Records:** Financial information, including transactions and invoices, is retained for a period of 7 years in accordance with HM Revenue and Customs (HMRC) requirements.
4. **Special Category Data:** Data considered as 'special category', such as health information or data concerning a person's race or ethnic origin, is only retained as long as is necessary for the specific purposes for which it was collected.
5. **CCTV Footage:** If applicable, CCTV footage is typically retained for a short period, not exceeding 30 days, unless it is being used for the investigation of an incident.

After the expiry of the retention period, personal data is securely deleted or destroyed. Anonymised data, which can no longer be associated with an individual, may be retained beyond these periods for statistical or research purposes.

Please note that in certain circumstances, we may lawfully retain data for longer periods, such as where we are required to do so in accordance with legal, regulatory, tax, or accounting requirements, or for safeguarding purposes.

We regularly review our data retention policies to ensure compliance with applicable laws and regulations and to ensure that data is not held longer than necessary.

You also have the right to ask us to delete your data (sometimes known as '*the right to be forgotten*').

COOKIES

A cookie is a small text file which is placed onto your computer (or other electronic device) when you access our website. If you use our website, we may use cookies to:

- Track your use of the site;
- Recognise you whenever you visit this website (this speeds up your access to the site as you do not have to log on each time);
- Obtain information about your preferences, online movements and use of the internet;
- Carry out research and statistical analysis to help improve our content, products and services and to help us better understand our visitor/customer requirements and interests
- Target our marketing and advertising campaigns more effectively
- Make your online experience more efficient and enjoyable

If you do not want to accept cookies, you can change your browser settings so that cookies are not accepted. If you do this, please be aware that you may lose some of the functionality of this website. For further information about cookies and how to disable them please go to: www.aboutcookies.org or www.allaboutcookies.org.

If you visit our website when your browser is set to accept cookies, we will interpret this as an indication that you consent to the use of cookies.

This includes cookies that are essential in order to enable you to move around the site and use its features and cookies that are not essential but gather information about your use of the site.

If you want detailed information from Get Safe Online on how to protect your information and your computers and devices against fraud, identity theft, viruses and many other online problems, please visit <http://www.getsafeonline.org>. Get Safe Online is supported by the UK Government and leading UK businesses.

For more information, please see our separate [Cookie Policy](#).

YOUR RIGHTS

If you are a resident of the UK, you have various rights under the GDPR, including the following rights:

- **Right to object:** If we are using your data because we deem it necessary for our legitimate interests to do so, and you do not agree, you have the right to object. We will respond to your request within 30 days (although we may be allowed to extend this period in certain cases). Generally, we will only disagree with you if certain limited conditions apply (e.g., legal obligations, vital interests, legitimate interests that override the individual's rights).
- **Right to withdraw consent:** Where we have obtained your consent to process your personal data for certain activities (for example, providing you with services), or consent to market to you, you may withdraw your consent at any time.
- **Data Subject Access Requests (SAR):** Just so it's clear, you have the right to ask us to confirm what information we hold about you at any time, and you may ask us to modify, update or delete such information. At this point we may comply with your request or, additionally do one of the following:
 - We may ask you to verify your identity, or ask for more information about your request; and
 - Where we are legally permitted to do so, we may decline your request, but we will explain why if we do so.
- **Right to erasure:** In certain situations (for example, where we have processed your data unlawfully), you have the right to request us to "erase" your personal data. We will respond to your request within 30 days (although we may be allowed to extend this period in certain cases) and will only disagree with you if certain limited conditions apply.
- **Right of data portability:** If you wish, you have the right to transfer your data from us to another data controller. We will help with this – either by directly transferring your data for you, or by providing you with a copy in a commonly used machine-readable format.

- **Right to lodge a complaint** with a supervisory authority: You also have the right to lodge a complaint with your local supervisory authority, details of which can be found below.

To exercise any of your rights concerning your information, please send an email to the following address: LTimbrell@srpa.co.uk.

We may ask you to provide us with proof of your identity. Please do not be offended; this may occur even if we know you. It is a requirement of the GDPR in some cases.

PUPILS AND PARENTAL RIGHTS

At Sir Robert Pattinson Academy, we understand that parents and carers have a keen interest in their children's education and progress. However, it is important to clarify the extent and limitations of parents' rights to access their children's academy information and files.

1. **Understanding Pupil Rights:** As pupils grow older and become more mature, they have a right to a degree of privacy and control over their personal information. This is particularly relevant for secondary school pupils. Therefore, the right to access personal information gradually shifts from the parent or carer to the child when they reach secondary school.
2. **Legal Obligations and Exceptions:** There are specific circumstances where the Academy is legally obliged to provide information to parents. For instance, under the Education (Independent School Standards) (England) Regulations 2010, academies are legally obliged to provide parents with an annual report on their child's attainment in the main subject areas. Outside of these statutory requirements, access to detailed academy files and personal information is not automatic.
3. **Pupil Consent:** In cases where the pupil is competent to make their own decisions, we will usually seek the pupil's consent to share detailed personal information with parents or carers. This approach respects the pupil's privacy and autonomy.
4. **Sensitive Information:** For sensitive information, particularly that which relates to the welfare or health of the pupil, the Academy will carefully consider the implications of sharing this information. The decision to disclose will be made in the best interests of the pupil, taking into account their age, maturity, and wellbeing.
5. **Parental Requests for Information:** Parents or carers who wish to request information about their child should contact the Academy directly. Each request will be considered individually, in line with our legal obligations and the pupil's rights and best interests. We may ask you to complete a form, which will include provision for procuring the pupil's consent.
6. **Transparency and Communication:** We are committed to maintaining open and transparent communication with parents and carers. While we may not be able to provide full access to all academy files, we endeavour to keep parents and carers informed about their child's progress and any significant concerns.

We encourage parents and carers to discuss any queries or concerns about access to information with us. Our priority is always the welfare and educational development of our pupils, balanced with respecting their rights to privacy and confidentiality.

REVIEW

This Policy was last reviewed in January 2026.

THE INFORMATION COMMISSIONER'S OFFICE

More information about privacy laws can be found at www.ico.org.uk.

Details of the UK supervisory authority: The Information Commissioner's Office. You can contact them in the following ways:

- Phone: 0303 123 1113
- Email: [casework@ico.org.uk](mailto:caserwork@ico.org.uk)
- [Live chat](#), via the ICO website
- Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Miss L Timbrell
Data Protection Officer
LTimbrell@srpa.co.uk
01522 882020