

Privacy Statement

Publication date: 01/05/2018

Last Review Date: July 2026

Review Frequency: Annually

Approved by:

Signed:



(Chief Executive Officer)

Michele Jolly

Signed:



(Chair of Board of Trustees)

Carol Liggins

Copies of this document can be made available in different formats.

Contents

Introduction	3
Statement Aims.....	3
Scope	3
Personal Data We May Collect About You	3
Keeping Your Information Up To Date	4
How We Collect Your Personal Data.....	4
Sources of Personal Information	5
Reasons We Collect And Use Your Personal Information	5
Marketing and Opting Out	8
Who Has Access To Your Personal Information?.....	9
Keeping Your Data Secure	9
Transferring Your Information Outside Of Europe	10
Information About Other Individuals	10
How long do we keep your data for?	11
Cookies.....	11
Third Party Liability	11
Children	11
Vulnerable Circumstances	11
Monitoring	11
Automated Decision Making.....	12
Your Rights	12
Exercising Your Data Protection Rights.....	12
How We Handle Rights Requests	13
Data Protection Complaints.....	13
The Information Commissioner's Office	14
Review of this Statement	14
Amendment History	14

Introduction

Age UK Lincolnshire, referred to in this Privacy Statement as “we”, “us” and “our”, is the data controller for the personal data we collect and use. This means that, under the UK General Data Protection Regulation and the Data Protection Act 2018, we decide how and why your personal data is processed.

We take privacy very seriously. We are committed to keeping your data secure and processing it fairly and lawfully. Please read this Privacy Statement carefully, as it explains the types of information we may collect and hold, how that information is used, who it may be shared with, and how you can contact us if you have any questions or concerns.

Statement Aims

This Privacy Statement explains how we collect, use, store and protect personal data. It applies whether you receive a service from us, contact us for information or advice, support us, volunteer for us, work for us, or use our website.

It is intended to help you understand what information we hold, why we hold it, how it is used, who we may share it with, how long we keep it, and the rights you have in relation to your information.

This Statement should be read alongside any service-specific privacy information we provide at the point we collect your data, which will give more detail about how information is used in particular circumstances.

Scope

We are Age UK Lincolnshire, a Registered Charity (1078539) with Company Registration Number 3777156 at 36 Park Street, Lincoln, LN1 1UQ.

For the purposes of the UK General Data Protection Regulation (“UK GDPR”) and the Data Protection Act 2018, we are the “data controller”. This means we decide how and why your personal data is used.

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 your personal information, we are responsible for how that information is managed. The UK GDPR and the Data Protection Act 2018 set out our obligations to you and your rights in relation to how we use 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.

Keeping Your Information Up To Date

It is important that the personal data we hold about you is accurate and current. Please let us know if your details change while you are in contact with us.

How We Collect Your Personal Data

We collect personal data in a number of ways, depending on how you interact with us. Most commonly, we receive information directly from you when you contact us, complete a form, speak to us by telephone, email us, engage with us face-to-face, make a donation, apply to work or volunteer with us, or otherwise choose to share information so that we can provide support.

In some circumstances, we also receive personal data from third parties. This may include referrals or information shared by partner organisations such as NHS bodies, local authorities, primary care providers, voluntary and community sector partners, carers, family members or others involved in supporting you. We only accept and use such information where it is lawful to do so and where it is necessary for the delivery or coordination of services.

When you visit or use our website, limited information may be collected automatically (typically technical information such as IP address and information about how the site is accessed and used). This helps us keep the website secure and improve it over time.

In the course of our work, the following types of data may be collected from you:

- **Identity Data** includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender.
- **Contact Data** includes address, delivery address, email address and telephone numbers.
- **Status Data** includes information about why you are being referred to a specialist organisation through our pathway. This may include health data where it is necessary and lawful for us to use it.
- **Financial Data** includes bank account and payment card details.
- **Technical Data** includes internet protocol (IP) address, your 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.
- **Enquiry Data** includes data you provided us with when you contact us with an enquiry.
- **Usage Data** includes information about how you use our website and services, as well as the frequency and pattern of your service use.
- **Marketing and Communications Data** includes your preferences in receiving marketing from us and our third parties and your communication preferences.
- **Anonymous Data** includes data that may be socio-demographic (for instance information about your work or profession, nationality, education) but also includes any combination of personal information identified above, including health information, but in a format from which you cannot be identified either directly or indirectly
- **Special Category Data** includes data regarding health conditions or data relating to protected characteristics such as race, ethnicity or sexual orientation
- **Criminal Offence Data** includes data relating to criminal convictions and offences, for example that may be revealed during a DBS check

Sources of Personal Information

We may collect personal data about you when you make an enquiry with us; apply for a job; apply to volunteer; interact with our personnel; receive a service from us; you are referred to us from a third party; visit or use our website; give us feedback; or complete a form and submit it to us.

We may collect data about you from third parties and publicly available sources. For example, we may collect personal information from:

- analytics providers or search information providers
- providers of technical, legal, accountancy, payment and delivery services and other specialist agencies
- social media platforms, where you interact with our social network pages, applications or content, or where you use one of our services that allows interaction with social networks.
 - interact with any of our social network pages or applications; or
 - you use one of our services that allow interaction with social networks, we may receive information relating to your social network accounts

We may collect information about you from the following sources:

1. **Information that you give to us:** this includes information you provide when using our website, submitting a form, calling us, emailing or writing to us, applying for a role with us, or visiting our offices or other premises. This may include special category data where relevant.
1. **Information we receive from other sources:** including other agencies providing services to you, medical professionals, our commissioning bodies such as local authorities and the NHS, HMRC, or from your friends and family and anyone holding attorney over your affairs – this may include Special Category Data
2. **Information we receive automatically:** this is mainly Technical and Anonymous Data

Reasons We Collect And Use Your Personal Information

We only process personal data where we have a lawful basis under the UK GDPR. Depending on the circumstances, this may include:

Consent – where you have given clear permission (for example, some types of marketing).

Contract – where processing is necessary to deliver a service to you or to manage employment or volunteering arrangements.

Legal obligation – where we must process data to comply with the law (for example, certain employment, safeguarding, tax or regulatory requirements).

Vital interests – where processing is needed to protect someone's life or prevent serious harm.

Legitimate interests – where we have a genuine and proportionate reason to use data to operate effectively as a charity, balanced against your rights and expectations.

Where we process special category data, such as health information, disability-related information, racial or ethnic origin, religious or philosophical beliefs, trade union membership, genetic or biometric data used for identification, sex life or sexual orientation, we will only do so where we have both a lawful basis under Article 6 UK GDPR and a separate condition

under Article 9 UK GDPR. We will identify and document the relevant Article 9 condition before using the data, make sure the processing is necessary and proportionate, and apply additional safeguards. Depending on the purpose, these safeguards may include restricted access, staff training, clear retention controls, data minimisation, secure storage, a data protection impact assessment where processing is likely to be high risk, and an Appropriate Policy Document where this is required under Schedule 1 of the Data Protection Act 2018.

Where we process criminal offence data, such as DBS information, information about criminal convictions, alleged offences, investigations, proceedings, cautions, sanctions or related security measures, we will only do so where we have a lawful basis under Article 6 UK GDPR and a specific condition under Schedule 1 of the Data Protection Act 2018, unless we are otherwise authorised by law. We will only process this information where it is necessary, relevant and proportionate, and we will not keep a comprehensive register of criminal convictions. We will document the condition relied on, use an Appropriate Policy Document where required, restrict access to those who need the information, retain it only for as long as necessary, and apply appropriate security and confidentiality safeguards.

The table below sets out the main reasons we use personal data and the legal bases we rely on.

Reason for using data	Type of data	UK GDPR lawful basis	Additional condition or safeguard where relevant
Responding to requests for information, advice, support or general enquiries	Identity, contact, enquiry, usage and, where necessary, special category data	Legitimate interests; contract where we are taking steps to provide or arrange a service; vital interests in urgent situations	Where health, care or other special category information is used, we will identify an Article 9 condition, such as health and social care purposes, safeguarding, equalities monitoring or substantial public interest, and apply appropriate safeguards.
Providing, managing or reviewing our services, including befriending, telecare, community connections, response services and other activities	Identity, contact, status, enquiry, financial, usage and special category data where necessary	Contract; legitimate interests; legal obligation where required by law; vital interests where necessary to protect life or prevent serious harm	Special category data will only be used where an Article 9 condition applies and the use is necessary and proportionate. We will document the condition relied on and apply additional safeguards where required.
Making onward referrals to partner services, health and social care organisations, emergency services	Identity, contact, status, enquiry and special category data where necessary	Consent where appropriate; legitimate interests; vital interests in emergencies; legal	Where special category data is shared, we will rely on an appropriate Article 9 condition and share only what is necessary.

or other agencies where appropriate		obligation where required by law	Safeguarding or emergency disclosures may be made without consent where this is necessary and lawful.
Recruiting, supporting and managing volunteers	Identity, contact, enquiry, status, financial, special category and criminal offence data where necessary	Legitimate interests; contract or steps before entering into an arrangement; legal obligation where required by law	DBS and criminal offence information will only be processed where lawful and necessary, with a relevant Schedule 1 condition and appropriate safeguards. Special category data will be handled under an Article 9 condition where required.
Recruiting, employing and managing staff	Identity, contact, enquiry, status, financial, special category and criminal offence data where necessary	Contract; legal obligation; legitimate interests	Employment-related special category data may be processed under Article 9 conditions such as employment, social security and social protection law, occupational health, equalities monitoring or substantial public interest. Criminal offence data will only be processed where lawful, necessary and safeguarded.
Processing donations, Gift Aid, invoices, payments, direct debits, refunds, payroll, pensions and other financial transactions	Identity, contact, financial, transaction and related enquiry data	Contract; legal obligation; legitimate interests	We will retain financial and Gift Aid records where required for accounting, audit, tax, fraud prevention and charity governance purposes.
Sending service updates, fundraising appeals, volunteering opportunities, campaign information, event invitations, supporter communications and other marketing	Identity, contact, marketing and communications data	Consent; legitimate interests where permitted, including postal marketing and electronic marketing under the charitable purposes soft opt-in where all legal	Electronic marketing will comply with PECR. We will give clear opt-out opportunities and honour marketing objections. Where we rely on legitimate interests, we will consider and document the balancing of our interests against

		requirements are met	individual rights and expectations.
Managing our website, IT systems, security, business continuity, records, reporting, analytics and service improvement	Technical, usage, identity, contact, anonymous and aggregated data	Legitimate interests; legal obligation where required; consent where required for non-essential cookies or similar technologies	We will use appropriate security controls, minimise the data used for reporting and analytics, and seek cookie consent where required.
Reporting to commissioners, funders, regulators, auditors, trustees and other bodies where necessary	Usage, anonymous, aggregated and, where necessary, limited identity or service data	Contract; legal obligation; legitimate interests	We will use anonymised or aggregated information wherever possible and share identifiable data only where necessary and lawful.
Handling complaints, incidents, safeguarding concerns, accidents, insurance matters, legal claims and governance responsibilities	Identity, contact, enquiry, service, incident, special category and criminal offence data where necessary	Legal obligation; legitimate interests; vital interests where necessary	Where special category or criminal offence data is used, we will identify the relevant Article 9 or Schedule 1 condition and apply safeguards, including restricted access and appropriate retention controls.

Marketing and Opting Out

We may contact you with information about our services, activities, fundraising, volunteering opportunities, campaigns, events and other ways to support our charitable work. We will do this only where we are permitted to do so by data protection and electronic marketing laws, including the UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations.

Where we send marketing by email, text message or other electronic message, we will rely on your consent unless another lawful route is available. From 5 February 2026, charities may also be able to use the charitable purposes soft opt-in. This means we may send electronic marketing without asking for fresh consent first where we collected your contact details directly from you, at or after that date, when you expressed an interest in our charitable purposes or offered support for them, and where the message is solely to further those charitable purposes. This may include updates about our work, fundraising appeals, volunteering opportunities, campaigns or events.

We will not use the charitable purposes soft opt-in unless we gave you a clear and simple opportunity to opt out when we collected your details, and we will include an easy way to opt out in every electronic marketing message. The soft opt-in will not be used for contacts collected before 5 February 2026 unless the legal requirements are met. Where the soft opt-in does not apply, we will ask for your consent before sending electronic marketing.

We may send postal communications where permitted by law on the basis of our legitimate interests, after considering your rights, interests and reasonable expectations. We may also

contact you by telephone where permitted by law and where you have not opted out or registered with a relevant preference service.

You can change your preferences or opt out of marketing at any time by using the unsubscribe or opt-out details provided in our communications, by emailing dpo@ageuklincolnshire.org.uk, or by writing to us at the address set out under “Your Rights”. We will act on your request promptly and will not make it difficult for you to withdraw consent or object to marketing.

Who Has Access To Your Personal Information?

We will not sell or rent your information to third parties. We will not share your information with third parties for marketing purposes. We may share personal data where necessary to deliver services safely and effectively and to meet our legal and contractual obligations. Where we do this, we share the minimum necessary and put appropriate safeguards in place. This may include:

- **Third Party Service Providers** working on our behalf: We may pass your information to our third-party service providers, agents, subcontractors and other associated organisations for the purposes of completing tasks and providing services to you on our behalf. However, when we use third party service providers, we disclose only the personal information that is necessary to deliver the service and we have a contract in place that requires them to keep your information secure and not to use it for their own direct marketing purposes.
- **Our website provider:** 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.
- **Our professional advisors and agents** for the purposes of advising and representing us in any matter connected with your account or your use of our website upon which we legitimately consider that advice or representation is needed.
- **Link Workers and Third Party Service Providers** as part of a referral pathway: This may include primary care network providers, NHS partnership organisations, voluntary sector organisations, PCN managers, clinical directors, and other healthcare and social care providers.
- **Your General Practitioner (GP):** As part of the NHS’s commitment to holistic healthcare provision, information about your pathway referral is provided to your GP so they can ensure they are offering you the best support. If you would prefer for your GP not to be provided with information about your referral pathway, please discuss this with our agent.

Please be reassured that we will not release your information to third parties for them to use for their own direct marketing purposes, unless you have requested us to do so, or we are required to do so by law, for example, by a court order or for the purposes of prevention of fraud or other crime.

Keeping Your Data Secure

We will use 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 keep paper records to a minimum, and destroy any temporary paper records once electronic systems have been updated. If we need to store paper records they are kept in secure environments;
- We train our staff in good records management;
- We provide data protection training and guidance to staff and volunteers;
- Where we use suppliers who process personal data on our behalf, we carry out appropriate checks and put written agreements in place that require them to keep data secure and use it only in line with our instructions.
- We have procedures in place to deal with suspected personal data breaches;
- Payment details are encrypted

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. Once we receive your information, we make our best effort to ensure its security on our systems. Where we have given (or where you have chosen) a password which enables you to access certain parts of our websites, you are responsible for keeping this password confidential. We ask you not to share your password with anyone.

Personal data may be stored on secure cloud-based systems operated by providers such as Microsoft 365, Salesforce and Sage, where those systems are used for our services, administration, finance, governance or records management.

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.

Transferring Your Information Outside Of Europe

We use reputable cloud and IT providers to store and process personal data (for example Microsoft 365, Salesforce and Sage). In some cases, this may involve personal data being stored or accessed outside the UK.

Where personal data is transferred outside the UK, we will ensure appropriate safeguards are in place to protect it. Depending on the circumstances, this may include the UK International Data Transfer Agreement (IDTA) and/or the UK Addendum to EU Standard Contractual Clauses, together with any required risk assessments and contractual controls.

If you would like more information about international transfers relevant to your data, please contact us using the details under “Your Rights”.

Information About Other Individuals

If you provide information to us about another person (for example, if you are supporting them to access a service), please ensure you have their permission to share that information with us, and only share what is necessary. If we need to contact them directly, we may provide them with privacy information so they understand how their data is used.

How long do we keep your data for?

As a general rule, we will not keep your data for any longer than is necessary to complete tasks or provide you with services. We have a separate policy setting out retention periods for specific types of data. You can ask to see this policy by writing to us, using the contact details under the “Your Rights” section below. You also have the right to ask us to delete your data in certain circumstances (sometimes known as ‘the right to be forgotten’.)

Cookies

Our website uses cookies and similar technologies. Cookies are small text files stored on your device that help websites function and can provide information about how a site is used.

We use cookies to help our website work properly, keep it secure, and understand how it is used so we can improve it. Where required, we will ask for your choices and you can manage your cookie preferences at any time using our cookie settings / cookie notice.

For more information, please see our Cookie Notice on the website.

Third Party Liability

Our website may link to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or use personal data. We do not control those websites or services and are not responsible for their privacy practices. We encourage you to read the privacy notice of any third-party website or service you use.

Children

Our services are primarily intended for adults and older people, but we may occasionally receive personal information relating to children or young people, for example where a family member, carer, volunteer, supporter, job applicant, website user or safeguarding matter is involved. Where we process children’s personal information, we will take extra care to make sure it is used lawfully, fairly and transparently, and only where necessary.

If you are under 13 and using our website or online services, please ask your parent or guardian before providing us with personal information. If you are aged 13 to 16, we encourage you to involve a parent or guardian where appropriate, particularly where you are asking us for support, making a donation, signing up to an event, volunteering, or sharing sensitive information. Where we need consent from a parent or guardian, or where safeguarding or capacity concerns apply, we will take reasonable steps to check that the right person has given permission.

Vulnerable Circumstances

We are committed to protecting people who may be in vulnerable circumstances, including supporters, service users and volunteers. We recognise that additional care may be needed when we use personal information in these situations, and we follow relevant good practice guidance in our interactions with people who may need extra support.

Monitoring

Records of interactions with us, including by email and telephone, may be monitored or recorded for training, quality assurance, complaint handling, safeguarding and service improvement. Where calls are recorded, we will tell you at the point of contact and we will not record payment card details.

Automated Decision Making

We do not use automated decision-making (including profiling) that produces legal effects or similarly significant effects for individuals in relation to our services. If this position changes and automated decision-making is used in a way that affects you, we will explain what is happening and your rights.

Your Rights

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.

Right to withdraw consent: Where we have obtained your consent to process your personal data for certain activities (for example, marketing), you may withdraw your consent at any time.

Data Subject Access Requests: You have the right to ask us whether we hold personal information about you and to request a copy of that information. You may also ask us to correct, update or delete information where the law gives you that right. We may ask you to verify your identity or provide more information so that we can respond to your request properly.

- 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 rectification: You have the right to ask us to correct personal information that is inaccurate or incomplete.

Right to restriction: In certain circumstances, you have the right to ask us to restrict how we use your personal information.

Right not to be subject to solely automated decisions: You have rights where a solely automated decision produces legal effects or similarly significant effects for you.

Right to complain: If you are unhappy with how we have processed your personal data, you have the right to complain to us. Please see the "Data Protection Complaints" section below.

Exercising Your Data Protection Rights

To exercise any of your rights concerning your personal information, please send an email to the following address:

DPO@ageuklincolnshire.org.uk

Or write to us at the following postal address:

Data Protection Officer
Age UK Lincolnshire
36 Park Street
Lincoln
LN1 1UQ

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

How We Handle Rights Requests

We will respond to a request to exercise your data protection rights without undue delay and, in any event, within one month of receiving it.

Where a request is complex, or you have made multiple requests, we may extend the time for responding by up to a further two months. If we do this, we will tell you within one month of receiving your request and explain why.

Where we are legally permitted to refuse a request, we will explain our reasons for doing so.

Data Protection Complaints

We are committed to protecting personal data and take all complaints about the handling of personal data seriously.

A data protection complaint is any expression of dissatisfaction about how we have handled personal data, including:

- concerns about insecure data handling;
- a failure to respond appropriately to a data protection rights request; or
- concerns that personal data has been processed unfairly or unlawfully.

If you wish to make a complaint, please use the contact details set out under “Exercising Your Data Protection Rights” above.

Please provide sufficient information to enable us to identify you and investigate your complaint, including:

- your name;
- your contact details; and
- full details of your complaint.

When we receive a data protection complaint, we will:

- acknowledge receipt of the complaint within one month;
- investigate the matters raised;
- provide a substantive response without undue delay; and
- keep a record of the complaint and any action taken, to help us monitor compliance and improve our services.

If you remain dissatisfied after receiving our response, you have the right to complain to the Information Commissioner’s Office (ICO), the UK’s supervisory authority for data protection matters. Details of how to contact the ICO are provided below.

The Information Commissioner's Office

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

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

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

Review of this Statement

This Privacy Statement is reviewed at least annually and may be updated sooner if our services, systems or legal obligations change. The latest version will always be available on our website.

Amendment History

Version Number	Effective Date:	Summary of Amendments	Author
v1.0	01/05/2018	Publication	Operations Director
v2.0	August 2019	Annual review. Updated policy following implementation of GDPR and Data Protection Act 2018 requirements. Expanded sections on data collection, lawful processing, data sharing, security, cookies, international transfers and individual rights.	Operations Director
v3.0	March 2023	Annual review. Rewritten as a Privacy Statement. Expanded categories of personal data, lawful bases for processing, service-specific processing activities, referral pathways, marketing, data sharing arrangements, cloud storage providers and data subject rights. Added detailed processing activities table and updated organisational information.	Corporate Services Director
v3.2	30/03/2023	Minor amendment to wording and content. Updated cookie section wording and minor drafting amendments following publication of v3.0.	Corporate Services Director
V4.0	January 2026	Annual review. Updated organisational name, contact details and UK GDPR content. Expanded sections on data collection, lawful processing, information sharing, marketing, international data transfers, security measures, data subject rights, and introduced new sections on children,	Corporate Services Director

		vulnerable circumstances, monitoring and automated decision-making.	
V4.1	July 2026	Comprehensive review and policy redesign. Improved policy structure and readability; strengthened provisions relating to special category and criminal offence data; enhanced lawful basis and safeguarding information; expanded marketing compliance requirements; revised processing activities table; updated systems, retention and security controls; and strengthened children's privacy, individual rights and governance provisions.	Corporate Services Director