Privacy Notice

This Privacy Notice applies to all websites, applications, services, programmes, events, and activities delivered by CyberSafe Scotland

CyberSafe Scotland is a registered company incorporated in Scotland under company number SC744691 and has a registered office at 214 Union Street, Aberdeen, AB10 1TL. All significant decisions about data processing and policy implementation will be made using UK GDPR (General Data Protection Regulation). This notice is set out to help you understand the types of data that we collect from you, and/or your business, and how that data is used and managed.

Commitment

CyberSafe Scotland is committed to protecting the privacy and security of your personal data. We continually monitor compliance through implementing policies & procedures to safeguard data and by setting regular reviews to manage these policies and procedures.

Data Controller

In accordance with ICO (Information Commissioners Office) requirements of Data Controllers (the main decision maker when it comes to how people's personal information is managed), CyberSafe Scotland is registered with the ICO (ZB429528). When you are using CyberSafe Scotland's website, CyberSafe Scotland is the Data Controller.

About Us

CyberSafe Scotland is a nonprofit organisation specialising in the development and delivery of tools to enable vulnerable children to safely navigate their online world. We provide data research to analyse need, and training and support to improve outcomes for children and young people in response. All income from our products and services is reinvested directly into providing further support for schools and families who cannot afford help.

Who we collect data from.

We collect personal data both directly from individuals and from third parties where this is necessary to deliver our services, fulfil safeguarding responsibilities, and meet our legal obligations

We collect personal information directly from:

- Children and young people participating in our programmes, workshops, or activities
- Parents, carers, or guardians
- Individuals who contact us for advice, support, or information
- Individuals attending training sessions or events
- Staff, volunteers, and job applicants

We may also receive personal information indirectly from:

- Schools, colleges, and other educational settings
- Local authorities and safeguarding partners
- Charities and third-sector organisations
- Professionals involved in supporting children and families (such as teachers or social workers)
- Referrers who signpost individuals to our services

In some cases, we may collect limited information from publicly available sources or partner organisations where this is necessary to support our work and safeguard individuals.

Privacy Notice

What data do we collect

We may collect, use, store and transfer different types of personal data depending on how you interact with us, including:

Personal details - This may include:

- Name
- Date of birth or age
- Contact details (such as email address, telephone number, and address)

Information about children and young people - Where we deliver programmes or provide support, this may include:

- Name and age of the child or young person
- School or educational setting
- Information shared during workshops, sessions, or support activities

Safeguarding and wellbeing information - In some circumstances, we may process more sensitive information where this is necessary to protect individuals. This may include:

- Information relating to a child or young person's wellbeing or safety
- Concerns about online harm, exploitation, or abuse
- Information provided by parents, schools, or safeguarding professionals

Special category data - Where necessary and appropriate, we may process special category data, such as:

- Health or wellbeing information
- Information relating to a person's background or circumstances where relevant to safeguarding

Education and professional information - For training and partnership work, this may include:

- Job role and organisation
- Professional contact details
- Records of attendance at training or events

Communication data

- Records of correspondence with us (emails, messages, or enquiries)
- Feedback or survey responses

Technical and usage information - When you use our website or digital services, we may collect:

- IP address
- Browser type and device information
- Information about how you use our website (via cookies or similar technologies)

We may also collect and use aggregated data (such as statistical or demographic data) for any purpose. Aggregated data does not directly or indirectly identify you and is not considered personal data. However, if we combine aggregated data with personal data so that you can be identified, we will treat it as personal data in accordance with this privacy notice.

Where we need to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter with you (e.g. to provide you with goods or services). In this case, we may have to cancel a product or service you have with us. We will notify you if this is the case at the time.

How and why we use your data

Privacy Notice

We use personal information to deliver our services, protect individuals, and meet our legal and regulatory responsibilities.

We use personal information for the following purposes:

Category	Purpose	How we use it	Lawful Basis
Children and young people	To deliver education and safeguarding services	Deliver workshops, programmes, and awareness sessions; engage during activities; respond to concerns; support online safety and wellbeing	Public Task / Legitimate Interests / Vital Interests (where required for safeguarding)
Parents, carers, and guardians	To support children and provide advice	Communicate about services; provide guidance and support; respond to enquiries; involve in safeguarding matters where appropriate	Legitimate Interests / Public Task / Legal Obligation
Schools, local authorities, and partner organisations	To deliver commissioned services and manage relationships	Coordinate delivery of programmes; share updates, reports, and feedback; manage contracts and partnerships	Contract / Legitimate Interests / Public Task
Individuals seeking advice or support	To respond to enquiries and provide assistance	Communicate via email or other channels; provide information, advice, and resources	Legitimate Interests
Training participants and event attendees	To organise and deliver training and events	Manage bookings and attendance; communicate event details; facilitate participation (including online platforms); gather feedback	Contract / Legitimate Interests / Consent (where appropriate)
Donors and supporters	To manage donations and support fundraising	Process donations; maintain records; communicate about fundraising activities (where appropriate)	Legitimate Interests / Consent
Staff, volunteers, and trustees	To manage our organisation and deliver services	Recruitment and onboarding; manage roles and responsibilities; maintain records; provide training and supervision	Contract / Legal Obligation / Legitimate Interests
Professional contacts and networks	To build partnerships and deliver services	Maintain relationships; communicate about opportunities, events, and collaborative work	Legitimate Interests
Website users	To provide and improve our website and services	Respond to enquiries; analyse usage; ensure security; manage website functionality (including cookies where applicable)	Legitimate Interests / Consent (for cookies where required)

Privacy Notice

Payment customers (individuals and organisations)	To process payments for services	Process transactions via third-party providers; maintain financial records; manage billing and invoicing	Contract / Legal Obligation
Safeguarding cases (any relevant individuals)	To protect individuals from harm	Assess and respond to concerns; share information with appropriate authorities where necessary	Public Task / Legal Obligation / Vital Interests
Service users, programme participants, stakeholders, and partner organisations	Research, monitoring, evaluation, impact measurement, and service improvement	Analyse service delivery, identify trends and emerging risks, evaluate programme effectiveness, monitor service quality, develop evidence-based services, and improve programmes, training, resources, and support activities	Legitimate Interests / Public Task (where applicable)
Service users, programme participants, stakeholders, and partner organisations	Audit, governance, reporting, and accountability	Produce anonymised and aggregated reports, support funding applications, fulfil audit, governance, compliance, and reporting requirements, and share anonymised findings with funders, partners, researchers, public bodies, government agencies, and other stakeholders where appropriate	Legitimate Interests / Public Task (where applicable)

Special category data - Where we process special category (sensitive) personal information, we rely on one or more of the following conditions:

- **Article 9(2)(g) - Substantial public interest (safeguarding) -** Processing is necessary for safeguarding children and individuals at risk, in line with UK data protection law.
- **Article 9(2)(c) - Vital interests -** Where it is necessary to protect someone's life or prevent serious harm and the individual is unable to give consent.
- **Article 9(2)(a) - Explicit consent -** Where appropriate, we may rely on explicit consent to process certain types of sensitive information.

Who are our stakeholders

Cyber afe Scotland works with a range of stakeholders to deliver our services and support children, young people, and communities.

Our stakeholders include:

Children, young people, and families, Education and childcare settings, Safeguarding and public sector organisations, Partner organisations, Funders and supporters, Staff and governance, Professional contacts and service providers

Privacy Notice

Protecting your personal information

We take the security of your personal information seriously and are committed to protecting it. We have appropriate technical and organisational measures in place to help prevent unauthorised access, loss, misuse, or disclosure of personal information. This includes secure website technology, password-protected systems, encryption of sensitive data where appropriate, and processes to detect, investigate, assess, and manage security incidents.

We regularly review and improve our security measures to ensure they remain effective and aligned with UK GDPR requirements and best practice.

If a personal data breach occurs that is likely to result in a risk to individuals' rights and freedoms, we will follow the relevant legal requirements, including notifying the Information Commissioner's Office (ICO) within 72 hours where required. We use ICO guidance when managing and responding to security incidents and will take appropriate steps to protect affected individuals and their information.

Retention

We only keep your personal data for as long as necessary to fulfil the purposes we collected it for, including to meet any legal, accounting, or reporting requirements. Retentions will vary depending on the type of data and our legal obligations. When we no longer need your information, we will securely delete or anonymise it. If you would like more detail about how we long, we keep specific types of information please contact us any time.

Who we share information with

We may share or receive personal information with trusted third parties where this is necessary to deliver our services, support children and families, manage our organisation, comply with legal obligations, protect individuals from harm, or fulfil contractual requirements.

Where third parties process personal information on our behalf, they act as our data processors and are subject to contractual obligations requiring them to process information only in accordance with our instructions and applicable data protection laws.

We take appropriate steps to ensure that all third parties maintain suitable confidentiality, security, and data protection standards.

We may share information with:

- Our staff, associates, volunteers, trustees, and contractors involved in delivering our services
- Schools, educational settings, local authorities, safeguarding partners, and public bodies where necessary to deliver services, support safeguarding activities, or meet legal obligations
- Partner organisations and organisations we collaborate with on projects, events, research, community initiatives, or funded programmes
- Organisations commissioned to assist with the delivery, coordination, administration, or hosting of workshops, training sessions, events, seminars, or digital resources
- IT, cloud hosting, website, data storage, cybersecurity, and business support providers
- Providers of communication and collaboration tools, including email, messaging, online meeting, and event management platforms

Privacy Notice

- Payment processors and financial service providers involved in processing payments, donations, invoicing, or financial administration
- Professional advisers, including legal, financial, accounting, insurance, audit, supervision, and governance advisers
- Funding bodies, commissioners, and organisations supporting our work where reporting, monitoring, evaluation, or compliance requirements apply
- Government bodies, regulators, law enforcement agencies, safeguarding agencies, and other authorities where disclosure is required by law or necessary to protect individuals from harm
- Organisations involved in organisational changes, mergers, acquisitions, restructuring, or the transfer of business assets
- Where an organisation commissions us to deliver a service, workshop, seminar, or event, we may share registration, attendance, participation, and feedback information with that organisation where this is necessary for delivery, reporting, evaluation, or contractual purposes.
- Where events, workshops, seminars, or online meetings involve multiple participants, attendees may be able to see information such as names, email addresses, profile information, meeting chat messages, questions, comments, or shared content as part of normal participation.
- We may share names, email addresses, photographs, job titles, and organisational information in connection with networking events, collaborative activities, promotional activity, or professional engagement where appropriate and lawful to do so.
- If a child, young person, or vulnerable adult is at risk of harm, we may disclose personal information to safeguarding agencies, local authorities, law enforcement, or other relevant authorities where necessary to protect individuals or comply with legal obligations.

We do not sell or rent personal information to third parties and do not share personal information with third parties for their own direct marketing purposes.

We only share the minimum information necessary for each purpose and take reasonable steps to ensure that personal information remains protected throughout its lifecycle.

Aggregated and anonymised data

We may create and use aggregated and anonymised information for research, service evaluation, impact measurement, trend analysis, reporting, funding applications, and to improve our services. We may share aggregated and anonymised information with funders, partner organisations, researchers, public bodies, and other stakeholders where this supports our charitable objectives.
We take reasonable steps to ensure that individuals cannot be identified from aggregated or anonymised information. Where information could reasonably identify an individual, it will be treated as personal data and protected in accordance with this privacy notice.

Website

CyberSafe Scotland collects personal data from web forms submitted by individuals requesting information in the form of general enquiries or to register for the events and services provided by

Privacy Notice

CyberSafe Scotland. This comprises the name, phone number, email address, mailing address, company name, subject & message of the person making the enquiry.

Our websites & information we share around services & involving stakeholders may contain links to other websites run by other organisations. This privacy policy applies only to our website, so we encourage you to read the privacy statements on the other websites you visit. We cannot be responsible for the privacy policies and practices of other sites even if you access them using links from our website. In addition, if you linked to our website from a third-party site, we cannot be responsible for the privacy policies and practices of the owners and operators of that third party site and recommend that you check the policy of that third party site.

Social Media

CyberSafe Scotland can be found on social media platforms such as Facebook, Instagram, YouTube, and LinkedIn. Social media is an important part of our awareness effort, so you may be presented with retargeting ads & emails in future following a visit to our website. We may target ads at audiences that we believe match the profile of our target audience and would therefore be interested in our services. We will also regularly tag or mention you where we are carrying out business promotion on your behalf or to raise your professional profile.

These platforms are run by commercial companies and CyberSafe Scotland is not the Data Controller or Data Processor of your social media profile. You should contact these social media platforms directly if you have concerns over how your personal data is being used and stored by them.

Payment data

CyberSafe Scotland may collect and process personal and financial information in order to receive payments for our services and activities.

Payments for services
We collect payments from:

- Individuals who book training sessions, workshops, or events
- Organisations that commission us to deliver services

For these purposes, we may process personal information including:

- Name
- Billing address
- Email address
- Payment and transaction information (such as payment references)

Payments are typically processed securely via third-party payment providers such as PayPal. We do not store or have access to full payment card details.

Donations and fundraising
In some cases, we may receive donations through third-party platforms or fundraising portals.

Where donations are made via these platforms, personal and financial information may be collected, including:

- Name
- Contact details (such as email address)
- Billing information
- Payment details

Privacy Notice

This information is processed securely by the relevant platform. CyberSafe Scotland does not have access to full payment details such as card numbers.

The processing of payment information is governed by Paypal's and the donation portals own Privacy Policies, which you can review on their website. It is important to familiarise yourself with their privacy practices to understand how they will handle your data.

Website visitor behaviour analytic software

We use software to collect analytic information on how website visitors engage with our website pages and content. We do this to understand how our website visitors use a website in order to provide an efficient user experience along with relevant information. This information is only processed in a way which does not identify individuals.

Google Analytics

We use Google Analytics to collect standard internet log information on visitor behaviour patterns. We do this to understand how our website visitors use a website in order to provide an efficient user experience along with relevant information. This information is only processed in a way which does not identify individuals. For more information about Google Analytics terms and conditions, visit https://www.google.com/analytics/terms/.

To opt out of being tracked by Google Analytics across all websites visit http://tools.google.com/dlpage/gaoptout.

We may also collect personal data from the website using Google Analytics to anonymously track how users interact with our site. This involves installing Google Analytics code on our website in the form of a 'cookie.' Cookies contain an ID number which is assigned to a user and provides us with the following information:

- Your IP address
- Your visits to our website
- The time of your visits and the length of time you spent on our website.
- The pages that you visited.
- Your location (although this might be influenced by the location of your server)
- The browser you are using.
- Type of operating system
- The device you are using (e.g., desktop, tablet or mobile)
- Referral source (how you arrived on our site, e.g. search engine, direct URL, social media, or third-party website).

The Principles

Whether we are acting as a data controller or processor we continue to apply the UK GDPR principles to all personal & Sensitive data that we hold, or process and these principles lie at the heart of our approach to processing personal data.

1) Processed lawfully, fairly and in a transparent manner in relation to individuals.

2) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes.

3) Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

4) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.

5) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.

6) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

International

We process personal data in accordance with UK GDPR and apply appropriate standards when making decisions about how your information is used, stored, and protected.

Personal data is primarily stored and processed within the UK. In some circumstances, information may be processed outside the UK, but within the European Economic Area (EEA), for example where we use trusted service providers, cloud-based systems, backup or disaster recovery arrangements, or where services are accessed from outside the UK. This may include situations where UK-based systems or servers are temporarily unavailable and secure contingency or failover systems hosted within the EEA are used to maintain service continuity and data availability.

Where personal data is transferred outside the UK, we ensure that appropriate safeguards are in place to protect your information and maintain your rights and freedoms. These safeguards may include UK adequacy regulations, the UK International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses, or other approved contractual and technical measures designed to ensure that personal data is protected to a standard equivalent to that required under UK GDPR.

We take a risk-based approach to international data transfers and do not transfer higher-risk or special category personal data outside the UK unless it is necessary to do so and appropriate protections are in place. Where required by law, we will obtain explicit consent before processing or transferring such information.

If you access or use our services while located outside the UK, your information may be transferred outside the UK where necessary in order to provide those services securely and effectively.

Your data protection rights.

Under data protection law, you have rights we need to make you aware of. The rights available to you depend on our reason for processing your information.

Your right of access - You have the right to ask us for copies of your personal information.

Your right to rectification - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances.

Your right to restriction of processing - You have the right to ask us to restrict the processing of your personal information in certain circumstances.

Privacy Notice

Your right to object to processing - You have the the right to object to the processing of your personal information in certain circumstances.

Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

Your right to complain - Under the **Data (Use and Access) Act 2025**, you have the right to complain if you believe your personal data has been handled inappropriately

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Where you have given, us consent to use your personal information in a certain way you have the right to withdraw that consent at any time. If you withdraw your consent, we may not be able to provide certain products or services to you. We will tell you if that is the case

Communications

The Privacy and Electronic Communication Regulations (PECR) sit alongside the Data Protection Act and the UK GDPR and gives individuals specific rights around electronic communication. This means if we send electronic marketing or use cookies or similar technologies, we must comply with both PECR and the UK GDPR

Although PECR covers a number of areas which provide public electronic communication network or services PECR applies to Cybersafe Scotland for

- Direct Marketing by phone, email, text, or fax
- Website cookies

Direct Marketing

You have the right to stop the use of your personal data for direct marketing activity through all channels, or selected channels. We must always comply with your request unless an exemption applies. There are several ways you can stop direct marketing communications from us.

- Click the “unsubscribe” link in any direct marketing email communication that we send you. We will then stop any further direct marketing emails.
- You can also email, call, or write to us to ask us to add you to our suppression list.

Exemptions

If you unsubscribe from our marketing mailing lists, you will still receive service & support communications from us where you are an existing customer, supplier or have a relationship with us that requires us to process your information as part of a contract or where the law requires us to do so.

Website Cookies

'Cookies' are small pieces of information sent by an organisation to your computer and stored on your hard drive to allow that website to recognise you when you visit. They collect statistical data about your browsing actions and patterns and do not identify you as an individual. example, we use cookies to store your country preference. This helps us to improve our website and deliver a better more personalised service. It is possible to switch off cookies by setting your browser preferences. Turning cookies off may result in a loss of functionality when using our websites.

Artificial Intelligence (AI)

Privacy Notice

We may use artificial intelligence (AI) to support our work and in some cases to demonstrate the dangers and in some cases to improve how we deliver services, always with care and oversight.

There are 3 types of AI we may use or test:

- Non-generative AI: - This type of AI helps with analysing and sorting data, such as identifying trends in anonymised service information. It does not create new content and does not make decisions on its own.
- Generative AI: -This type of AI can produce content such as draft letters, summaries or reports based on information it is given. When used, it supports staff and is never a replacement for human judgement.
- AI agents (agentic AI): -This type of AI can carry out multi-step tasks on behalf of users, such as retrieving information, interacting with systems, or completing defined workflows. AI agents may use generative or analytical AI as part of their process, but they operate only within clearly defined instructions and permissions set by staff.

No solely automated decision-making

We do not make decisions about individuals based solely on automated processing where those decisions have legal or similarly significant effects. All decisions that affect individuals involve meaningful human involvement.

Right to challenge decisions

Where AI-supported processes contribute to decisions affecting individuals, those individuals have the right to request human review, challenge the outcome, and receive an explanation of how the decision was reached, where applicable.

Contact Us

Cybersafe Scotland
214 Union Street
Aberdeen
AB10 1TL

info@cybersafescotland.org

Regulatory Information

Further information around your rights can be found at https://ico.org.uk/your-data-matters

The ICO's address:

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