SENSECERE CIC

04 – SENSECERE GENERAL DATA PROTECTION REGULATION (GDPR) POLICY

Date of Policy Issued/Review	**NOVEMBER 2020 / REVIEWED 1ST MAY 2026**
Director / Management	**Sharon Wilson / Rachel Grimshaw**

POLICY STATEMENT

This policy is in response to the new GDPR which came into effect on 25 May 2018. The GDPR replaces the Data Protection Act (1994) and whilst broadly similar in principle, requires a review and update on how Sensecere handles and stores personal data.

REFERENCES

a. Data Protection Act 2018
b. Guide to GDPR
c. ICO Information Commissioner's Office.

Children have the same core data protect rights as adults, including:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

GENERAL POLICY

- Sensecere will record requests they may receive verbally.
- Sensecere will understand when they can refuse a request and are aware of the information they will need to provide to individuals when they do so.
- Sensecere will have processes in place to ensure that they will respond to a request for rectification without undue delay and within one month of receipt.
- Sensecere are aware of the circumstances when they can extend the time limit to respond to a request.

SHARING INFORMATION FOR CHILD SAFEGUARDING PURPOSES.

Considerations:

- Be clear about how data protection can help you share information to safeguard a child.
- Identify your objective for sharing information you need to safeguard a child.
- Develop clear and secure policies and systems for sharing information.
- Be clear about transparency and individual rights.
- Assess the risks and share as needed.
- Enter into a data sharing agreement.
- Follow the data protection principles.
- Share information using the right lawful basis.
- Share information in an emergency.

RIGHT TO BE INFORMED

Sensecere will provide individuals, staff, and parents/carers with all the following privacy information:

- The name and contact details of our organisation.
- The contact details of our data protection officer (DPO).
- The purposes of the processing.
- The lawful basis for the processing.
- The categories of personal data obtained (If the personal data is not obtained from the individual it relates to).
- The recipients or categories of recipients of the personal data.
- The details of transfers of the personal data to any third countries or international organisations.
- The retention periods for the personal data.
- The rights available to individuals in respect of the processing.
- The right to withdraw consent (if applicable).
- The right to lodge a complaint with a supervisory authority.
- The source of the personal data (if the personal data is not obtained from the individual it relates to).
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
- The details of the existence of automated decision-making, including profiling (if applicable).

- Sensecere will provide individuals with privacy information at the time personal data is collected from them.
- If Sensecere obtains personal data from a source other than the individual it relates to, Sensecere will provide them with privacy information within a reasonable of period of obtaining the personal data and no later than one month.
- If Sensecere plans to communicate with the individual, at the latest, when the first communication takes place; or
- If Sensecere will plan to disclose the data to someone else, at the latest, when the data is disclosed.

Sensecere will provide the information in a way that is:

- Concise.
- Transparent.
- Intelligible.
- Easily accessible; and
- Uses clear and plain language.

Sensecere will regularly review and, where necessary, update our privacy information. If Sensecere plans to use personal data for a new purpose, they will update their privacy information and communicate the changes to individuals before starting any new processing. Sensecere will periodically undertake an information audit to find out what personal data is held and what they do with it.

THE RIGHT OF ACCESS

- Sensecere will know how to recognise a subject access request and will understand when the right of access applies.
- Sensecere will understand the nature of the supplementary information they will need to provide in response to a subject access request.
- Sensecere will have processes in place to ensure that they will respond to a subject access request without undue delay and within one month of receipt.
- Sensecere will are aware of the circumstances when they can extend the time limit to respond to a request.
- Sensecere will understand that there is a particular emphasis on using clear and plain language if they are disclosing information to a child.
- Sensecere will understand what they will need to consider if a request includes information about others.

THE RIGHT TO RECTIFICATION

- Sensecere will know how to recognise a request for rectification, and they will understand when this right applies.
- Sensecere will have appropriate systems to rectify or complete information or provide a supplementary statement.
- Sensecere will have procedures in place to inform any recipients if they rectify any data, they have shared with them.

THE RIGHT TO ERASURE

- Sensecere will know how to recognise a request for erasure, and they will understand when the right applies.
- Sensecere will understand that there is a particular emphasis on the right to erasure if the request relates to data collected from children.
- Sensecere will have procedures in place to inform any recipients if they erase any data they have shared with them.
- Sensecere will have appropriate methods in place to erase information.

THE RIGHT TO RESTRICT PROCESSING

- Sensecere will know how to recognise a request for restriction, and they will understand when the right applies.
- Sensecere will have appropriate methods in place to restrict the processing of personal data on our systems.
- Sensecere will have appropriate methods in place to indicate on our systems that further processing has been restricted.
- Sensecere will understand the circumstances when they can process personal data that has been restricted.
- Sensecere will have procedures in place to inform any recipients if they restrict any data they have shared with them.
- Sensecere will understand that they will need to tell individuals before they lift a restriction on processing.

THE RIGHT TO DATA PORTABILITY

- Sensecere will know how to recognise a request for data portability, and they will understand when the right applies.
- Sensecere can transmit personal data in structured, commonly used, and machine-readable formats.
- Sensecere will use secure methods to transmit personal data.

THE RIGHT TO OBJECT

- Sensecere will know how to recognise an objection, and they will understand when the right applies.
- Sensecere will have clear information in our privacy notice about individuals' right to object, which is presented separately from other information on their rights.
- Sensecere will understand when they will need to inform individuals of their right to object in addition to including it in our privacy notice.
- Sensecere will have appropriate methods in place to erase, suppress or otherwise cease processing personal data.

RIGHTS IN RELATION TO AUTOMATED

DECISION MAKING AND PROFILING

Sensecere is, and will, not be required to conduct automated decision making and profiling. Should the requirement for this process come forward, this policy will be required to be updated and approved by the Committee and updated privacy guidelines given to all parties affected prior to the operation taking place.

ACCOUNTABILITY AND GOVERNANCE

- Sensecere will take responsibility for complying with the GDPR, at the highest management level and throughout our organisation.
- Sensecere will keep evidence of the steps Sensecere will take to comply with the GDPR.
- Sensecere will put in place appropriate technical and organisational measures, such as:

    - adopting and implementing data protection policies (where proportionate);
    - taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;
    - putting written contracts in place with organisations that process personal data on our behalf;
    - maintaining documentation of our processing activities;
    - implementing appropriate security measures;
    - recording and, where necessary, reporting personal data breaches;
    - carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
    - appointing a data protection officer (where necessary); and,
    - adhering to relevant codes of conduct and signing up to certification schemes (where possible).

DOCUMENTATION

- Sensecere will document all the applicable information under Article 30(1) of the GDPR.
- Sensecere will document all the applicable information under Article 30(2) of the GDPR.
- Sensecere will document our processing activities in writing.
- Sensecere will conduct regular reviews of the personal data they process and update our documentation accordingly.

    - do information audits to find out what personal data our organisation holds;
    - distribute questionnaires and talk to staff across the organisation to get a more complete picture of our processing activities; and,
    - review our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

When preparing to document processing activities Sensecere will:

- do information audits to find out what personal data our organisation holds;
- distribute questionnaires and talk to staff across the organisation to get a more complete picture of our processing activities; and,
- review our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

As part of our record of processing activities Sensecere will document, or link to documentation, on:

- information required for privacy notices;
- records of consent;
- controller-processor contracts;
- the location of personal data;
- Data Protection Impact Assessment reports; and
- records of personal data breaches.
- Sensecere will document processing activities in electronic form so they can add, remove and amend information easily.

SECURITY

- Sensecere will undertake an analysis of the risks presented by our processing and use this to assess the appropriate level of security they will need to put in place.
- When deciding what measures to implement, Sensecere will take account of the state of the art and costs of implementation.
- Sensecere, when processing children's data especially sensitive information or when sharing sensitive information will conduct a Data Protection Impact Assessment will be carried out and used.
- Where necessary, Sensecere will have additional policies and ensure that controls are in place to enforce them.
- Sensecere will make sure that they regularly review our information security policies and measures and, where necessary, improve them.
- Sensecere understands that they may also need to put other technical measures in place depending on our circumstances and the type of personal data Sensecere will process.
- Sensecere will use encryption and/or pseudonymize where it is appropriate to do so.
- Sensecere will understand the requirements of confidentiality, integrity and availability for the personal data they process.
- Sensecere will make sure that they can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.
- Sensecere will ensure that any data processor they use also implements appropriate technical and organisational measures.
- Sensecere will know how to recognise a personal data breach.
- Sensecere will understand that a personal data breach isn't only about loss or theft of personal data.
- Sensecere will have prepared a response plan for addressing any personal data breaches that occur.
- Sensecere will have allocated responsibility for managing breaches to a dedicated person or team.

- • Our staff will know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.
- Sensecere will know who the relevant supervisory authority for our processing activities is.
- Sensecere will have a process to notify the Information Commissioner's Office (ICO) of a breach within 72 hours of becoming aware of it, even if Sensecere does not have all the details yet.
- Sensecere will know what information they must give the ICO about a breach.
- Sensecere will have a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.
- Sensecere will know they must inform affected individuals without undue delay.
- Sensecere will know what information about a breach they must provide to individuals, and that they should provide advice to help them protect themselves from its effects.
- Sensecere will document all breaches, even if they don't all need to be reported.

SUMMARY

Data protection is primarily based around common sense and decency. The data obtained by Sensecere will be used solely for the purpose of running the play scheme and no other purposes. All data processes will be conducted by staff or committee who are trusted and aware of the criteria to be met in this policy.

ASSOCIATED POLICY's

- Safeguarding Children Policy
- Confidentiality Policy
- Complaints Policy
- Equality & Diversity Policy
- Left Behind Child Policy
- Administration of Medication

Version Narrative

Version No	Date	Comments	Name
V1.0	Nov 2020	Original Document	Sharon Wilson