SPIRIT STUDIOS.

Data Protection Policy

Last reviewed: 14/08/2023

Table of contents

Introduction

Everyone has rights regarding the manner in which their personal data is handled. International consistency around data protection laws and rights is crucial both to businesses and organisations, and to individuals. Having clear laws with safeguards in place is more important than ever given the growing digital economy, and this is what the General Data Protection Regulation (GDPR) legal framework aims to provide. Fines for infringement of GDPR can be up to 4% of global turnover or 20 million Euros, whichever is greater.

During the course of our activities Spirit Studios will collect, store and otherwise process personal information about a variety of individuals with whom we have (or have had) contact.

This policy is supplemented by guidance documents which must also be adhered to as part of this policy. This supplementary guidance is designed to complement the policy and help those subject to the policy to comply with its requirements on a practical level. The guidance will be updated as and when necessary.

A glossary of terms used throughout this policy is included in Appendix 1.

Scope of the Policy

This policy sets out Spirit Studios' requirements regarding data protection and the legal conditions which must be satisfied in relation to the processing of personal data. Processing includes obtaining, recording, holding, altering, disclosing, destroying or otherwise using personal data.

The types of data that we may be required to handle include details of current, past and prospective employees and students and their family members, suppliers, school contacts and any others with whom we communicate. This information may be held on paper or electronically on a computer, server or other media, and is subject to certain legal safeguards specified in the GDPR and other regulations. The GDPR sets out how that information should be processed, and imposes restrictions on how we may use it.

Policy Statement

Spirit Studios takes its responsibilities under the GDPR and the requirement to treat personal information in an appropriate and lawful manner very seriously and as such complies with the data protection principles, as set out in this policy.

Responsibilities

This policy applies to all employees, including temporary, casual, contract and agency staff, as well as any contractors or service providers acting on behalf of Spirit Studios.

The Director has overall responsibility for ensuring Spirit Studios complies with the GDPR legal framework and with this policy. The Director is supported in this responsibility by the other members of senior management. Any questions or concerns about the operation of this policy should be referred in the first instance to dpo@spiritstudios.ac.uk

This policy is reviewed annually. Recommendations for any amendments should be reported to dpo@spiritstudios.ac.uk for consideration as part of the review process. Spirit Studios will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

Data Protection Principles

Employees processing personal data must comply with the six data protection principles. These are principles of good practice and compliance is a requirement of the GDPR, which is enforced by the Information Commissioner. The principles require that personal data must be:

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

   The GDPR is not intended to prevent the processing of personal data, but to ensure that it is done fairly, transparently and without adversely affecting the rights of the data subject.

   For personal data to be processed lawfully, a legal basis for processing must be identified. This legal basis will have an effect on the individual's rights. For example, if we rely on someone's consent to process their data, they will generally have stronger rights, i.e. the right to have their data deleted. The legal bases available include:

- Consent of the data subject

- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of a data subject or another person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

  The data subject must be told who the data controller is (for most of our purposes, this will be Spirit SSR Ltd), the purpose for which the data are to be processed and the identities of any other third countries (Non-EU) or international organisations to whom the data may be disclosed or transferred. This information must be provided to the data subject in a privacy notice at the time the data is collected or if this is not possible, then as soon as is practicable.
  When special categories of data are being processed (i.e. sensitive personal data, such as ethnicity or medical information), an additional condition must be met:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law
- Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
- Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- Processing relates to personal data manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards

- Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes

If something is a legitimate mandatory or legal requirement, data subjects should not be asked for consent and given the impression that they have a choice if this is not the case. Advice from the Data Protection Officer (dpo@spiritstudios.ac.uk) should be sought on consent issues and before processing sensitive personal data.

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 considered incompatible with the initial purposes.**

   Personal data may only be processed for the specific purposes notified to the data subject via the privacy notice when the data was first collected or for any other purposes specifically permitted under the GDPR. Personal data must not be further processed in a manner which is incompatible with these purposes. This means that personal data must not be collected for one purpose and then used for an entirely different, unrelated purpose. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs, unless an exemption from this requirement applies. It may be the case that you cannot use the personal data for another purpose unless the data subject consents. Advice should be sought from the Data Protection Officer (dpo@spiritstudios.ac.uk).

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

   Personal data held about data subjects must be sufficient for the purposes for which it is held. Information which is not needed or is not relevant for a

purpose must not be collected or otherwise processed. The minimum amount of personal data needed to properly achieve the purpose in question should be identified and collected; additional, excessive personal data must not be held.

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.**

   Personal data must be accurate and, where necessary, kept-up-to-date. Information which is incorrect or misleading is not accurate; steps must be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards.

   Personal information identified as being factually inaccurate must be amended or erased; however, it may not be appropriate to erase this information altogether if historic decisions have been based on it. In these cases, the information must be amended for future use with an explanatory note placed on file as required to explain the situation. Where a data subject disagrees with a professional opinion about him or herself which does not – by definition – constitute a verifiable fact, the data subject's difference of opinion will be noted on the file in the relevant places.

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 GDPR in order to safeguard the rights and freedoms of individuals.**

   Personal data must not be kept longer than is necessary for the purpose for which it is being processed. This means that data must be securely destroyed or erased from our systems when it is no longer required, i.e. there is no legal requirement to retain it and there is no business or operational need for the information.

   Personal information should be managed with the company's Data Retention Schedules, which provides guidance on how long certain types of

information should be retained, and when and how they should be destroyed.

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.**

   From the point of collection of personal data to the point of destruction, we must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

   Maintaining personal data security means, amongst other things, guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised to use data can access it.
- Integrity means that personal data must be accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users must be able to access the data if they need it for authorised purposes. Personal data must therefore be stored on the company's secure network with appropriate access controls, and not on individual computers, laptops or other devices such as phones, tablets, CDs or memory sticks.

Security procedures include:

- Vigilance. Any stranger seen in non-public areas must be questioned (if safe to do so) or reported to the police.
- Entry Controls. Buildings, offices or other secure areas must be locked when empty or not in use. Entry codes must not be shared with unauthorised individuals and keys and fobs must be kept secure.
- Secure lockable desks and cupboards. Desks, cupboards and filing cabinets are kept locked if they hold confidential information of any kind. It should always be assumed that personal data is confidential, although there may be cases where it is not.
- Methods of disposal. Paper documents containing personal information must be securely shredded before being disposed of through a secure waste service. They must not be discarded with regular waste or recycling material.

Electronic data or media, such as USB sticks, CDs, DVDs, etc. must be wiped or destroyed securely to ensure that the information is no longer accessible or recoverable. Hardware and devices such as laptops, PCs, smartphones, etc. must be cleaned and/or securely disposed of by the technical department to ensure the information stored on them is no longer accessible or recoverable.

- Equipment. Data users must ensure that individual monitors are positioned in suitable locations to ensure that confidential information is not visible to passers-by or other unauthorised individuals, e.g. through office windows or doors. Users must lock their PCs and other devices when left unattended, even for a few minutes, to prevent unauthorised access to systems. At the end of each day, users must log out of systems and shut down machines to maintain security and enable essential system updates to be installed. Fax machines must be in secure locations where received faxes are not accessible to unauthorised individuals. Portable equipment such as smartphones, laptops, tablets, or removable media such as USB sticks, CDs etc., must be kept secure at all times and not left unattended in cars, on public transport or in public areas.
- Preventing disclosure to unauthorised third parties. Personal data must not be disclosed to unauthorised third parties intentionally or through negligent actions. Personal data must not be disclosed to third parties unless it has been verified that they have authority to access that information. Care must be taken when transmitting personal data, e.g. by email or fax, to ensure it is addressed correctly, marked appropriately, e.g. 'private and confidential,' and is only sent to the intended recipient.

Individual's Rights

Personal data must be processed in line with the data subject's rights. Data subjects have:

The right to be informed. The right to be informed encompasses our obligation to provide 'fair processing information', typically through our privacy notice. It emphasises the need for transparency over how we use personal data.

The right of access. Under GDPR, individuals have the right to obtain confirmation that their data is being processed; access to their personal data; and other supplementary information.

The right to rectification. Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. If we have disclosed the personal data

in question to third parties, you must inform them of the rectification where possible. We must also inform the individuals about the third parties to whom the data has been disclosed where appropriate. Rectification requests must be responded to within one month. This can be extended by two months where the request for rectification is complex.

The right to erasure. The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which is was originally collected/processed
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR)
- The personal data has to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child.

We can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- Archiving purposes in the public interest, scientific research, historical research or statistical purposes.
- The exercise of defence of legal claims.

If we have disclosed the personal data in question to third parties, we must inform them about the erasure of personal data, unless it is impossible or involves disproportionate effort to do so.

The right to restrict processing. Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, we are permitted to store the personal data but not further process it. We can retain just enough information about the individual to ensure that the restriction is respected in future. We will be required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, we should restrict the processing until we have verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interest), and we are considering whether our organisation's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If we have disclosed the personal data in question to third parties, we must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so. We must inform individuals when we decide to lift a restriction on processing.

The right to data portability. The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- To personal data an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When the processing is carried out by automated means

Personal data must be provided in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

The data must be provided free of charge.

If the individual requests it, we may be required to transmit the data directly to another organisation if this is technically feasible. However, we are not required to adopt or maintain processing systems that are technically compatible with other organisations.

If the personal data concerns more than one individual, you must consider whether providing the information would prejudice the rights of any other individual.

Responses must be made without undue delay, and within one month. This can be extended by two months where the request is complex or where a number of requests are received. We must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

When we decide not to take action in response to a request, we must explain why to the individual, informing them of their right to complain to the Information Commissioner and to a judicial remedy without undue delay at the latest within one month.

The right to object. Individuals have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- Direct marketing (including profiling)
- Processing for purposes of scientific/historical research and statistics.

If we process personal data for the performance of a legal task or our organisation's legitimate interests, individuals must have an objection on 'grounds relating to his or her particular situation'. We must stop processing the personal data unless we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims.

If we process personal data for direct marketing purposes, we must stop processing personal data for marketing purposes as soon as we receive an objection. There are no exemptions or grounds to refuse. Such an objection must be dealt with at any time and free of charge.

If we process personal data for research purposes, individuals must have 'grounds relating to his or her particular situation' in order to exercise their right

to object. If we are conducting research where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing.

If our processing activities fall into any of the above categories and are carried out online, we must offer a way for individuals to object online.

Rights related to automated decision making and profiling. The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

Individuals have the right not to be subject to a decision when it is based on automated processing and it produces a legal effect or a similarly significant effect on the individual. We must ensure that individuals are able to obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it. This right does not apply if the decision:

- Is necessary for entering into or performance of a contract between you and the individual
- Is authorised by law (e.g. for the purposes for fraud or tax evasion prevention)
- Based on explicit consent

GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their performance at work, economic situation, health, personal preferences, reliability, behaviour, location or movements.
When processing personal data for profiling purposes, we must ensure that appropriate safeguards are in place, including:

- Ensure that processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences.
- Use appropriate mathematical or statistical procedures for the profiling.
- Implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions taken must not:

- Concern a child

- Be based on the processing of special categories of data unless:
    - We have the explicit consent of the individual
    - The processing is necessary for the reasons of substantial public interest on the basis of EU/Member State law. This must be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard fundamental rights and the interests of the individual.

Accountability and Governance

The GDPR includes provisions that promote accountability and governance. We must demonstrate that we comply with the data protection principles. We must:

- Implement appropriate technical and organisational measures that ensure and demonstrate that we comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.
- Maintain relevant documentation on processing activities
- Where appropriate, appoint a data protection officer
- Implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
    - Data minimisation
    - Pseudonymisation
    - Transparency
    - Allowing individuals to monitor processing
    - Creating and improving security features on an ongoing basis
- Use data protection impact assessments where appropriate

Documentation

As well as our obligation to provide comprehensive, clear and transparent privacy notices (see Individual's Rights), we are required to maintain records of activities related to higher risk processing, such as:

- Processing personal data that could result in a risk to the rights and freedoms of an individual; or
- Processing of special categories of data or criminal convictions and offences.

We must maintain internal records of processing activities. We must record the following information:

- Name and details of our organisation (and where applicable, of other controllers, your representative and data protection officer)
- Purpose of processing
- Description of the categories of individuals and categories of personal data
- Categories of recipients of personal data
- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place
- Retention schedules
- Description of the technical and organisational security measures.

We may be required to make these records available to the Information Commissioner for purposes of an investigation.

Data protection by design and by default

Under GDPR, we have a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into our processing activities.

We must take an approach to projects that promote privacy and data protection compliance from the start. For example:

- Building new IT systems for storing or accessing personal data
- Developing legislation, policy or strategy that have privacy implications
- Embarking on a data sharing initiative
- Using data for new purposes

This will ensure potential problems are identified at an early stage, when addressing them will often be simpler and less costly.

Data Protection Impact Assessments

Data protection impact assessments (DPIAs) (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

We must carry out a DPIA when we:

- Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
- Process special category data or criminal offence data on a large scale.
- Systematically monitor a publicly accessible place on a large scale.
- Use new technologies.
- Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
- Carry out profiling on a large scale.
- Process biometric or genetic data.
- Combine, compare or match data from multiple sources.
- Process personal data without providing a privacy notice directly to the individual.
- Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
- Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
- Process personal data which could result in a risk of physical harm in the event of a security breach.

A template Data Protection Impact Assessment form is available.

Data Protection Officer (DPO)

Any organisation is able to appoint a DPO. Whilst the GDPR doesn't oblige a small company like us to appoint a DPO, we must ensure that our organisation has sufficient staff and skills to discharge our obligations under the GDPR. Such obligations include:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- To be the first point of contact for the Information Commissioner and for individuals whose data is processed (employees, customers, etc.).

Transfer of Data

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined. Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

Transfers on the basis of a Commission decision

Transfers may be made where the commission has decided that a third country, a territory or one or more specific sectors in a third country, or an international organisation ensures an adequate level of protection.

Transfers subject to appropriate safeguards

You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individual's rights must be enforceable and effective legal remedies for individuals must be available following the transfers. Adequate safeguards may be provided by:

- A legally binding agreement between public authorities or bodies;
- Binding corporate rules (agreements governing transfers made between organisations within a corporate group);
- Standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- Standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority approved by the Commission;
- Compliance with an approved code of conduct approved by a supervisory authority;
- Certification under an approved certification mechanism as provided for in the GDPR;
- Contractual clauses agreed authorised by the competent supervisory authority; or
- Provisions inserted into administrative arrangement between public authorities or bodies authorised by the competent supervisory authority.

The GDPR limits organisations' ability to transfer personal data outside the EU where this is based only on the organisation's assessment of the adequacy of the protection afforded to the personal data.

Authorisations of transfers made by Member States or supervisory authorities and decisions of the Commission regarding adequate safeguards made under the Directive will remain valid/remain in force until amended, replaced or repealed.

The GDPR provides derogations from the general prohibition on transfers of personal data outside the EU for certain specific situations. A transfer, or set of transfers, may be made where the transfer is:

- Made with the individual's informed consent;
- Necessary for the performance of a contract between the individual and the organisation or for the pre-contractual steps taken at the individual's request;
- Necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- Necessary for important reasons of public interest;
- Necessary for the establishment, exercise or defence of legal claims
- Necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
- Made from a register which under the UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

The first three derogations are not available for the activities of public authorities in the exercise of their public powers.

Even where there is no Commission decision authorising transfers to the country in question, if it is not possible to demonstrate that individuals' rights are protected by adequate safeguards and none of the derogations apply, the GDPR provides that personal data may still be transferred outside the EU. However, such transfers are permitted only when the transfer:

- Is not being made by a public authority in the exercise of its public powers;
- Is not repetitive (similar transfers are not made on a regular basis);
- Involves data related to only a limited number of individuals;
- Is necessary for the purposes of the compelling legitimate interests of the organisation (provided such interests are not overridden by the interests of the individual); and

- Is made subject to suitable safeguards put in place by the organisation (in the light of an assessment of all the circumstances surrounding the transfer) to protect the personal data.

In these cases, organisations are obliged to inform the relevant supervisory authority of the transfer and provide additional information to individuals.

Employees must seek guidance from senior management (dpo@spiritstudios.ac.uk) before transferring personal data overseas.

Using Data Processors

There may be times when employees want or need to use the services of a data processor. Personal data must only be transferred to a data processor if that data processor agrees to comply with the Spirit Studios' security and data protection procedures and policies or if they put in place equivalent measures themselves, which we deem to be acceptable.

Data processors must only be used if the processing is carried out under a contract made or evidenced in writing, where that contract states that the data processor is to act only on instructions from Spirit Studios as the data controller and requires the data processor to comply with equivalent technical and organisation security measures.

Telephone Enquiries

Any employee dealing with telephone enquiries must be aware of security requirements and ensure that personal data held by Spirit Studios is not disclosed inadvertently or inappropriately. This applies whether the purpose of the call is a formal requirement for information or an everyday enquiry. 'Blaggers' can target organisations which hold large amounts of personal data in an attempt to obtain information by deception and employees must be aware of the need to have appropriate security measures in place to prevent this, particularly during telephone calls. In particular, employees must:

- Check the caller's identity to make sure that information is only given to or discussed with a person who is entitled to it, e.g. if a caller says they are acting on behalf of a student and asks for an update on a complaint, check that the student has authorised us to liaise with the caller and that the caller is who they say they are; or if a student or employee calls asking

about their own information, ask security questions to verify that they are who they say they are.

- Make appropriate security checks if a caller is asking to be provided with personal data. To maintain the security of personal data, employees should suggest that the caller puts their request in writing if they are unsure about his or her identity and whether or not they are entitled to the information. See Individual's Rights for further information.
- Always ask the police and other callers to put their request in writing to the Data Protection Officer (dpo@spiritstudios.ac.uk) if they are making a formal request for disclosure of personal information.

Children's Personal Data

Consent needs to be obtained from a parent or guardian to process a child's data when providing any 'information society service' (i.e. target online services). The GDPR states that parental/guardian consent for access to online services is required for children aged 16 and under.

'Information society services' includes most internet services provided at the user's request and for remuneration. The GDPR emphasises that protection is particularly significant where children's personal information is used for the purposes of marketing and creating online profiles.

There are extra requirements when the request for erasure relates to children's personal data, reflecting the GDPR emphasis on the enhanced protection of such information, especially in online environments.

If we process the personal data of children, we should pay special attention to existing situations where a child has given consent to processing and they later request erasure of the data (regardless of age at the time of the request), especially on social networking sites and internet forums. This is because a child may not have been fully aware of the risks involved in the processing at the time of consent.

Formal Requests for Personal Data

Dealing with subject access requests

The GDPR gives individuals the right to access all the personal data a data controller processes about them, and Spirit Studios will assist individuals wishing to make a subject access request. Individuals are entitled to be provided with any information which constitutes their personal data unless the information is exempt. These requests must be dealt with in line with the provisions of the GDPR and company policy and employees should seek advice where necessary.

Subject access requests can be made verbally or in writing. Any employee who receives a subject access request directly from another individual must forward it to dpo@spiritstudios.ac.uk without delay. The request will then be recorded and logged before sending to the appropriate department or service for action.

No personal data will be provided in response to a subject access request until we are satisfied as to the identity of the data subject.

A copy of the information must be provided free of charge. However, we can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. A reasonable fee may also be charged to comply with requests for further copies of the same information. This does not mean we can charge for all subsequent access requests. The fee must be based on the administrative cost of providing the information.

Information must be provided without delay and within one calendar month of receipt of the subject access request. This can be extended by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of receipt of the request and explain why the extension is necessary.
Where requests are manifestly unfounded or excessive, in particular because they are repetitive, it is possible to refuse to respond. We must explain why to the individual, informing them of their right to complain to the Information Commissioner and to a judicial remedy without undue delay and at the latest within one month.

The subject access request may state specific data that the data subject wishes to receive. If a data subject wishes to have a copy of all personal data we store on them, documentation such as the Location of Personal Data may assist in the process.

A Subject Access Request letter is available in the '15. Subject Access Request' folder in the GDPR documentation. Whilst we should recommend individuals complete this form, it isn't compulsory. Any completed forms should be emailed to dpo@spiritstudios.ac.uk directly by the individual or forwarded by the

member of staff who received it. Such requests must be entered into the 'Individual's Rights' spreadsheet in the GDPR documentation.

Dealing with requests from third parties for disclosure of information

Third party organisations or individuals, such as solicitors, the police, DWP, local authorities, NHS or insurance companies may make requests to Spirit Studios for personal information which we hold. This could be information about a student, an employee or other third party, e.g. someone caught on CCTV footage. In these cases, the third party will be asking for information about an individual but they are not acting on that person's behalf. Spirit Studios will only consider such requests when they are made in writing and no personal data will be disclosed unless it can be disclosed in compliance with the GDPR. All such requests must be dealt with by the Data Protection Officer and must not be responded to by other employees directly without taking advice. Employees receiving such requests from external third parties must direct them to put their request in writing to the Data Protection Officer (dpo@spiritstudios.ac.uk).

Employees must not be pressured into disclosing personal data. They must refer to their line manager and/or the Data Protection Officer for advice if they are unsure whether or not it is appropriate to disclose information.

Requests to opt-out of Marketing

An individual can ask us to stop processing their personal data for direct marketing at any time. This includes any profiling of data that is related to direct marketing.

This is an absolute right and there are no exemptions or grounds for us to refuse. Therefore, when we receive an objection to processing for direct marketing, we must stop processing the individual's data for this purpose.

However, this does not automatically mean that we need to erase the individual's personal data, and in most cases it will be preferable to suppress their details. Suppression involves retaining just enough information about them to ensure that their preference not to receive direct marketing is respected in future. This would be true for an ex-student, where they may want us to keep limited information so we can provide any necessary support in the future: job references, new copies of certificates etc. We should ask if the individual wishes

us to erase their personal data if they were not affiliated with Spirit Studios in any way except to receive direct marketing.

Individuals can object to their data being processed or request it be erased verbally or in writing. We should recommend individuals contact us for such requests by emailing opt-out@spiritstudios.ac.uk with sufficient details to prove their identity. However this isn't compulsory and we must deal with such requests no matter how we receive them.

We have one calendar month to process the request. If you have doubts of the identity of the individual, you can request further information to verify their identity. Only request additional information that is necessary. Such requests for further information must be made without delay and within one month of the individual's initial request. We don't need to comply with the request until we have received the necessary information.

Once a request has been received and verified, it must be added to the 'Individual's Rights' spreadsheet in the GDPR documentation. The Marketing opt-out procedure must then be followed, updating the Individual's Rights spreadsheet when complete.

New Processes of Projects Involving the Use of Personal Data

If a member of staff wishes to introduce a new process or project involving the use of personal data, we need to ensure it is compliant with the General Data Protection Regulation (GDPR). To do this, the member of staff will complete the 'New Personal Data Process Request Form' and return it to dpo@spiritstudios.ac.uk. The information provided will be reviewed, suggestions made if necessary and then approved or rejected. The information provided will allow us to fulfil our legal requirements, such as creating/updating our privacy notices, documenting our legal basis for the processing, ascertain whether we need to undertake a Data Protection Impact Assessment (DPIA) and update and update our GDPR documentation.

Using Personal Data for Personal Matters

Employees and other data users must not use company-controlled personal data for their own purposes. Employees and other data users are in a position

of trust and must not abuse that position to access personal information for non-company purposes. Employees and other data users must access or otherwise process personal data only for company business purposes and not for personal curiosity or any other unofficial purpose.

Any person who knowingly or recklessly obtains or discloses personal information without the company's consent is committing a criminal offence under the GDPR.

Breach Notification

The GDPR introduces a duty on all organisations to report certain types of data breach to the Information Commissioner, and in some cases to the individuals affected.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

If you have caused or become aware of an actual or suspected personal data breach, you must immediately inform your line manager and complete the Personal Data Breach Report Form and send it to dpo@spiritstudios.ac.uk. This will facilitate decision making about whether senior management needs to notify the Information Commissioner or the public.

Details of any breaches need to be documented internally using the 'Personal Data Breach documentation – Template' form.

Negligent, reckless or deliberate breaches of this policy – whether it results in the notification of the Information Commissioner or not - will be treated seriously by Spirit Studios and will be subject to a full investigation. Any investigation may result in disciplinary action or dismissal, where appropriate.

If you are concerned that this policy has not been followed in respect of personal data about yourself or others, you should raise the matter by emailing dpo@spiritstudios.ac.uk.

Notifying the Information Commissioner (Senior Management only)

The Information Commissioner will have to be notified of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed, such a breach is likely to have a significant detrimental impact on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

This has to be assessed on a case by case basis. For example, we will need to notify the Information Commissioner about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly. A 'high risk' means the threshold for notifying individuals is higher than for notifying the Information Commissioner.

The following information must be included in a breach notification:

- The nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned; and
    - The categories and approximate number of personal data records concerned;
- The name and contact details of the data protection officer (if applicable) or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

A notifiable breach has to be reported to the Information Commissioner within 72 hours of the organisation becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows organisations to provide information in phases. A completed copy of the 'personal-data-breach-report-form-web-dpa-2018.doc' must be sent to casework@ico.org.uk with 'Personal data breach notification' in the subject field.

If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay.

Failing to notify a breach when required to do so can result in a significant fine up to 20 million Euros or 4 percent of the organisation's global turnover.

GDPR Review

Spirit Studios will perform an annual review of its GDPR documentation. This will involve data audits and documents being reviewed by the applicable departments.

Data Audit/Document	**Departments to Review**
Data Protection Officers Data Audit	Senior Management
Emergency Contact Data Audit	Admin
Experience Attendee Data Audit	Admin, Marketing
Job Applicant Data Audit	Senior Management
School Contacts Data Audit	Marketing
Staff Data Audit	Senior Management, Technical, Admin, Tutors
Student Data Audit	Senior Management, Technical, Admin, Tutors, Marketing
Supplier Data Audit	Senior Management, Technical, Marketing
UCAS Applicant Data Audit	Admin, Marketing
Visitor Data Audit	Technical
Website User and Enquirer Data Audit	Marketing
Enquiry Capture Form	Marketing
Staff Induction Form	Senior Management

Student Induction Form	Admin, Tutors, Senior Management
Student Bursary Application	Admin
Marketing Opt-Out Procedure	Marketing

Departments will pay particular attention to the following areas of each data audit:

- Any additional fields of personal data now being stored, how it was collected, who has access and where it is stored.
- Any additional processes - list the process name and description. Senior Management will decide on the legal basis for processing.
- Any additional special category data
- Any changes to our Data Retention Policies
- Any transfers to third countries or international organisations.

Additions/changes to a copy of a Data Audit should be done with a red font for additions and red strikethrough for anything to be removed.

From these amended data audits, senior management can then update:

1.Purposes of Processing
2.Categories of Individual, Personal Data and Recipients
4.Details of Transfers to Third Countries
5.Data Retention Schedules
7.Legitimate Interests Assessments
8.Privacy Notices
9.Records of Consent
10.Location of Personal Data
11.Data Protection Impact Assessments
13.Information Required for Processing Special Category Data.
14.Contact Details

In addition, the following will be reviewed by Senior Management:

- Ensure each transfer to third countries/international organisations is still protected.
- 6. Description of Technical and Organisational Security Measures
- 14. Contact Details
- Data Protection Policy
- Staff Training

Annotated documents made throughout the review process are to be stored in the '16. Review Policy' folder.

Appendix 1: Glossary of Terms

Data	Information which is stored electronically (on any media), on a computer (including in emails) or in most non-electronic filing systems or other manual records
Personal data	Data relating to a living individual who can be identified from that data (or from that data and other information in our possession or likely to come into our possession). Personal data can be factual (such as name, address, date of birth) or it can be opinion (such as aspects of an employment reference). Information can be personal data without including a person's name. Personal data may also be referred to as 'personal information'.
Sensitive personal data	Information about a person's: ● Racial or ethnic origin; ● Political opinions; ● Religious or similar beliefs; ● Trade union membership; ● Physical or mental health or condition; ● Sexual life; or information about ● The commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in any such proceedings. Sensitive personal data can only be processed under strict conditions and will usually require the explicit consent of the person concerned.

Processing	Any activity which involves the data. It includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing and destroying it. Processing also includes transferring personal data to third parties.
Data subject	The individual the data relates to and for the purpose of this policy, data subjects include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.
Data controller	An organisation or person who determines the purposes for which and the manner in which any personal data are, or are to be, processed. A data controller must be a 'person' recognised in law i.e. individuals, organisations and other corporate and unincorporated bodies of persons. Spirit SSR Ltd is a data controller.
Data processor	Any individual or organisation which processes personal data on behalf of a data controller. Employees of a data controller are not considered to be data processors, however the definition is likely to include suppliers or service providers which handle personal data on a data controller's behalf.
Data user	Includes employees and other staff members whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times
Privacy notice	A statement provided to data subjects when or before their personal data is collected which explains who the data controller is, what their information will be used for, to whom it may be disclosed for these purposes (particularly any external third parties) and any other information they may need to know in order to ensure that the processing is fair.
Information Commissioner	An independent regulator who reports directly to Parliament. The information Commissioner is responsible for regulating and enforcing the GDPR in the

	UK and provides advice and guidance about compliance to organisations and members of the public.