Data Protection Policy

In delivering its services Creative will need to collect and process certain types of information about people including staff, students and suppliers or providers of services to it. All such processing is subject to the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. This policy sets out Creative's intentions in fulfilling its obligations under this legislation.

Creative needs to keep personal information secure, but it goes much wider than appropriate security and requires a comprehensive approach to the collection, use, sharing and retention of personal information in order to build public confidence. Combined with the reliance on fast changing ICT capabilities and storage of vast amounts of data, it is essential that Creative has this overarching document which makes clear to the public Creative's approach to data protection and data sharing and explains the rights of the individual in relation to the information we hold about them. Publishing a clear and explicit policy and having the right approach to raising awareness and skills of staff, as they handle personal information, will be regarded as an integral element in promoting trust in the way Creative handles the personal data entrusted to it.

We have all been made aware of high-profile data breaches, and many will be aware of the Information Commissioner's powers to fine authorities up to 10 million euros for severe breaches. Many of the reported breaches are however simply down to human error, such as emailing the wrong recipient or not checking personal data before it is posted, leaving sensitive documents in the car or not checking a person's identity over the phone. These errors can all be avoided by officers and members of staff taking extra care in going about their duties and treating others' personal information as they would their own. Directors also have an important role to play in proper oversight of its systems and processes, so it makes breaches less likely.

Personal information promise

We, Alison Matthias and Darren Martin, Directors, on behalf of Creative promise that we will:

1. Value the personal information entrusted to us and make sure we respect that trust.

2. Go further than just the letter of the law when it comes to handling personal information and adopt good practice standards.

3. Consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems.

4. Be fair, open and transparent with individuals about how we use their information and who we give it to.

5. Make it easy for individuals to access, correct and request erasure (where we have no reason to retain), of their personal information.

6. Keep personal information to the minimum necessary and delete it when we no longer need it.

7. Have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands.

8. Provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or do not look after personal information properly.

9. Put appropriate resources into looking after personal information to make sure we can live up to our promises.

10. Regularly check that we are living up to our promises.

Signed:

Dated:

Introduction

Creative shall comply with its duties under the Data Protection Act 2018 and the rights of privacy and respect for personal and family life set out in Article 8 of the Human Rights Act 1998 at all times.

The Data Protection Act 2018 (the Act) places legal obligations on organisations who collect and use personal information and gives individuals certain rights. In addition, there are stricter requirements in the Act in respect of processing 'special category data'. Personal information can be held in any format for example, electronically, paper records, or photographic images, and the Act applies irrespective of how the information is held.

Responsibility for the Act

Creative is committed to ensuring all staff and contractors comply with the Act. Creative has an appointed Data Protection Officer – Alison Matthias, who is responsible for ensuring compliance with the Act.

There is a separate policy in respect of the Freedom of Information Act. Where a request is received under the FOIA or the EIRs but in fact it falls within the Data Protection regime, Creative will automatically channel it through the appropriate policy, as it is required to do, as different exemptions and therefore, different legal rights apply in the circumstances.

Scope

This policy applies to all personal information held in any recorded format such as email, paper, video or photographic images and applies to all staff who process personal data on behalf of Creative. It is a criminal offence to destroy personal information when the purpose of the destruction was to avoid disclosure following a request.

Adhering to the 6 principles of the Act

The Data Protection regime is underpinned by 6 certain fundamental principles, which form a code for the proper processing of personal data. Processing means anything we do with data, such as obtaining, copying, disclosing, altering, retaining or destroying information. If we cannot comply with all 6 of these principles, we should not be processing the data. The principles are summarised in the following diagram:

6 DATA PROTECTION PRINCIPLES

1. Personal data must be lawfully, fairly and transparently processed

2. Personal Data shall be collected for specified, explicit and legitimate purposes

3. Personal data shall be adequate, relevant and limited to what is necessary

4. Personal data must be accurate and up to date

5. Personal Data shall be kept in a form which permits identification for no longer than necessary

6. Personal data shall be held ensuring appropriate security

Creative will ensure that:

- It has procedures in place for complying with the six principles.
- Training on our data protection duties shall be mandatory for all staff. All new staff receive appropriate data protection training on induction and that refresher training and guidance is provided periodically, so that they understand that they are contractually responsible for complying with the law and know how to process information in accordance with these 6 principles.
- Advanced level training is provided to those members of staff who deal with highly sensitive personal information. Training needs mapping will be conducted, to identify those who require regular advanced training on data protection and information sharing to enable them to share with confidence.
- Everyone managing and handling personal information is individually and collectively responsible for compliance with this policy.
- A failure to follow this policy may result in disciplinary action or even criminal prosecution in the case of a wilful and deliberate breach.
- That individuals are informed of the purposes for which their data will be used and that consent is sought for such use, where required under the Act. Examples of model privacy notices are attached as an appendix to this policy.
- All staff are trained to recognise a subject access request and what to do about one.
- All appropriate, technical and organisational security measures to safeguard personal information will be put in place including encrypting or ensuring increased security settings of removable devices such as laptops or mobile phones and restricting the use of USB sticks in line with Creative's Information Security Policy.
- All staff are required to report data security breach incidents, including 'near misses' to the director.

Individual's rights

Creative will ensure that individuals can exercise their rights as set out in the Act including:

- The right to be informed of the purposes of the processing.
- The categories of personal data being processed.
- The right of subject access to their personal information.
- Who will or is likely to receive their information.
- The envisaged period for which the data will be stored.
- The right to prevent processing of personal information in certain circumstances.
- The right to rectify, block, erase, restrict, object or correct inaccurate information.
- The right to lodge a complaint.

These rights apply to all living, identifiable individuals on whom the school processes personal information.

Subject Access Requests

Article 15 of the GDPR provides the right for individuals to be told by the data controller (the organisation who determines the purposes for which and the way personal information is processed):

- If we hold information about them.
- To ask what we use it for.
- To be given a copy of the information.
- To be given details of other organisations or people we disclose it to.
- To ask for incorrect data to be corrected.
- To ask us not to use personal information about them for direct marketing.
- To be compensated for damage or distress if we do not comply with the Act.
- To object to decisions made only by automatic means – for example, where there is no human involvement.
- To ask the Information Commissioner's Office to investigate and assess whether we have breached the Act.

Creative will supply this information providing the request is made verbally or in writing, and it is sufficiently clear what personal information is being sought; therefore, sufficient information should be given by the applicant to enable Creative to locate the information requested.

There is no fee applicable, and Creative should respond within one month, unless the request is complex or multiple, in which case it may be extended by two further months. Creative will inform the applicant if it is extending the time frame in such circumstances setting out the reasons as to why.

Creative will respond to such requests within one month, unless the request is manifestly unfounded or excessive. There is no definition within the Act, but in respect of an 'excessive' request, it is generally taken to mean that the effort the organisation would have to expend in complying with the requirement to provide a copy is disproportionate to the benefit to be derived by the individual in receiving it. In such circumstances, Creative will refuse the request.

Advice should be sought from the Creative's data protection officer in the first instance, ideally before Creative commence their search and collation of the data.

Applicants should be aware that, if possible, they should resist submitting a subject access request during the school summer holidays as responding within the one month timeline may be an issue.

Where the individual makes a request electronically, Creative will provide the information in a 'commonly used electronic format' in accordance with GDPR, unless the applicant requests otherwise.

A request for personal information should be submitted the following contact: alison@creativeinexcellence.co.uk

What if the data includes information about other people?

Applicants will not automatically be given access to parts of their information which also identify other people, without that third party's agreement, even if they are related. Disclosure will depend on the context and whether information is already within knowledge and all the circumstances of the case. Seek advice if in doubt.

The Act says that Creative would not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

- The other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information, Creative must take into account all of the relevant circumstances, including:

- The type of information that would be disclosed.
- Any duty of confidentiality owed to the other individual.
- Any steps taken to seek consent from the individual.
- Whether the other individual is capable of giving consent.
- Any express refusal of consent by the individual.

These areas should be considered, but they are not necessarily determinative as the decision is one for Creative to make, balancing the data subject's rights against other individual rights.

This does not apply to staff whose name may appear within a person's information, it is expected that this will be disclosed unless there is a risk of 'serious harm'. The serious harm test is a legal test and advice should be sought. The GDPR provides that it is expected that Creative professionals will be disclosed.

What about requests for information about children or young people?[1]

All the rights set out in the paragraph above are equally applicable. However, it should be remembered that even if a child is too young to understand the implications of the subject access rights, it is still the right of the child rather than anyone else such as a parent or guardian. So, it is the child who has a right of access to the information held about them,

[1] Extracted from the ICO guide to the GDPR 22nd March 2018.

even though in the case of young children these rights are likely to be exercised by those with parental responsibility.

Before responding to a subject access request for information held about a student, Creative should consider whether the student is mature enough to understand their rights. If Creative is confident that the student can understand their rights, it should respond directly to the student. Creative may allow the parent/carer to exercise the student's rights on their behalf if the student authorises this, or if it is evident that this is in the best interest of the student.

What matters is that the student is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, Creative should consider, (in no particular order) among other things:

- The student's level of maturity and their ability to make decisions like this.
- The nature of the personal data.
- Any court orders relating to parental/carer access or responsibility that may apply.
- Any duty of confidence owed to the student.
- Any consequences of allowing those with parental responsibility access to the student's information. This is particularly important if there have been allegations of abuse or ill treatment.
- Any detriment to the student if individuals with parental responsibility cannot access this information.
- Any views the student has on whether their parents/carers should have access to information about them.

In Scotland there is a presumption that a person 12 years and over is of sufficient age and maturity, unless the contrary is shown. The law in Wales does not specify an age and competence is assessed depending on the level of understanding of the child, but it does indicate an approach that will be reasonable.[2]

Exemptions

Creative may also, under the Act and Article 15 GDPR, refuse disclosure of data under the right of access provisions, where the serious harm test is met in respect of disclosure of education data.

[2] The test on Gillick competency is also helpful in the context of data protection requests.

Information Sharing

Information sharing is a complex area spanning many statutes and often the detail is hidden in secondary legislation (such as orders or statutory instruments). Decisions on whether to share information must be taken on a case-by-case basis and therefore could not be a blanket policy statement to follow as this is likely to be unlawful. In addition, understanding what can legally constitute 'consent' is also fundamental.

However, the following statements should clarify previous common myths or misunderstandings regarding information sharing:

The Data Protection Act does not prevent, neither should it be seen as a barrier, to lawful information sharing.

Creative is not legally required to have an 'Information Sharing Protocol' in place, in order to share. The lack of an ISP should not be a reason for not sharing information that could help a practitioner deliver services to a person.

Consent is not a prerequisite to information sharing – but several legal regimes (including the Data Protection Act) confirm that the obtaining of valid consent will permit information to be shared lawfully, but you may be able to rely on other grounds to share rather than obtain consent.

Confidentiality you may owe to an individual, can, and in some circumstances, *must* be overridden, such as concerns that a vulnerable adult or child may be at risk of serious or significant harm. Follow the relevant procedures without delay.

Attached as Appendix 2 are seven golden rules for information sharing reproduced from the HM Government publication 'Information Sharing: Guidance for practitioners and managers'. The golden principles are equally relevant in Wales and provide staff with clear guidelines when they decide to share information.

Requests from third parties (e.g. the police) for an individual's personal information

Occasionally Creative may receive formal requests under the Act from other agencies or third parties such as the police, DWP or HMRC, solicitor firms etc. to physically access or receive a copy of the information relating to an individual. These sections do not provide Creative with an automatic reason to disclose, as is explained below.

The Act deals with several situations in which personal data is processed for the following 'crime and taxation' purposes:

- The prevention or detection of crime.
- The capture or prosecution of offenders.

- The assessment or collection of tax or duty.

The personal data could be disclosed if the disclosure is for any of the above crime or taxation purposes and the above purposes are 'likely to be prejudiced' if Creative did not disclose for example to the police or the Inland Revenue. The threshold for disclosure in these circumstances needs to be more than a mere risk of prejudice and needs to be a significant and weighty chance of prejudice to the above purposes. In such circumstances you would need the third party to set out what information they wanted to see (or envisaged) and what legal powers they are relying on and evidence of identity.

Disclosure of personal information over the telephone or face to face without establishing the identity of the recipient should be avoided.

What about our external suppliers and the school outsourcing personal data processing?

Creative uses third party organisations to perform some of its functions. Where such 'outsourcing' arrangements involve the processing of personal data, certain legal obligations are placed on the school to ensure this supplier looks after the personal information in the same secure way as Creative does. These obligations are more onerous now under GDPR than under the old data protection legislation therefore extra care needs to be taken when entrusting a third-party supplier with personal data. Seek advice if you are in doubt.

It is a legal requirement that the obligations imposed on the supplier (known as the data processor) is set out in a written contract or letter.

Introduction of new systems that affect personal information – what should Creative consider?

In developing information systems, new business processes or changing our existing processes that involve personal information, it is now a requirement to carry out a Data Protection Impact Assessment (DPIA) and to build in privacy-friendly solutions as part of modernising or introducing new systems. This is referred to under the GDPR as 'Privacy by Design and Default' and the DPIA can be a useful tool to help identify risks, help the school manage those risks and where possible, eliminate them.

The Council has standard templates for carrying out DPIAs, so you have an audit trail of how you have considered the impact of the new system on people's personal data. These are available on the Business Improvement and Modernisation section of the intranet.

Email use

School staff should only use an authorised email account to communicate in respect of school business and functions. Under no circumstances should school staff (including fixed term, temporary, supply, agency or otherwise) use their personal email account to communicate with pupils, to protect all individuals concerned. Any staff member communicating in breach of this policy may face disciplinary action.

Data security breaches

All data security breaches, including 'near misses', must be reported to the line manager responsible, who shall immediately inform the director, who shall advise on the necessary steps that need to be taken to contain any resultant damage and inform individuals who may be affected. A central record of all breaches will be retained, and serious breaches must now

be reported to the Information Commissioner's Office. There is a standard breach notification form on their website. The school's 'data security breach policy' should be consulted. A flowchart is set out in Appendix 4.

Oversight arrangements and review of policy

This policy will be reviewed annually. Compliance with this policy and related procedures will be monitored by the school leadership team and the governing body.

Complaints

A review of Creative's decision to *withhold* personal information where an applicant has made a subject access request can be made to the company's Data Protection Officer, Alison Matthias, who will facilitate a review. If the decision is upheld and the applicant remains unsatisfied, they may appeal to the Information Commissioner's Office.

Contact details:
Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel 01625 545745
www.informationcommissioner.gov.uk

Key Contact details:

- Wales Accord on the Sharing of Personal Information
  The WASPI team is currently hosted by the health authority and their contact details are available on their website www.waspi.org

Appendices

Appendix 1

Privacy Notice

The categories of pupil information that we process include the following non-exhaustive list:

- Personal identifiers and contacts (such as name, contact details and address)
- Characteristics (such as ethnicity, language, and free school meal eligibility)
- Safeguarding information (such as court orders and professional involvement)
- Special educational needs
- Medical and administration (such as doctors' information, child health, dental health, allergies, medication and dietary requirements)
- Attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- Assessment and attainment
- Behavioural information
- Food allergies

Why we collect and use pupil information

We collect and use pupil information, for the following purposes:

a) To support pupil learning
b) To monitor and report on pupil attainment progress
c) To provide appropriate pastoral care
d) To assess the quality of our services
e) To keep children safe (food allergies, or emergency contact details)
f) To communicate effectively with parents and carers.
g) To enable pupils to move from one educational setting to another seamlessly, or where we have co-operation arrangements with other schools for delivery of local curricular entitlements.

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing pupil information will usually be the following:

- As data controller, we use the information received for the purposes listed above to enable us to carry out data processing necessary for the performance of a task carried out in the public interest and in the exercise of official authority or where we have a legal obligation to process.

- In addition, concerning any 'special category data', where the processing is necessary for reasons of substantial public interest, or where we have obtained explicit consent.

How we collect pupil information

We collect pupil information via admission forms or registration forms. Whilst the majority of pupil information you provide to us is mandatory, some of it requested on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if you have a choice in this.

How we store pupil data

We hold pupil data securely for the set amount of time shown in our data retention schedule. We are required to retain certain educational information until a pupil's 25th birthday.

Who we share pupil information with

We routinely share relevant pupil information with the local authority.

Why we regularly share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so. Where appropriate we will aim to have a formal Information Sharing Protocol in place and have made a commitment to developing these in accordance with national standards laid down by the Welsh Government's Wales Accord on the Sharing of Personal Information (WASPI). See www.waspi.org

Youth support services

We also pass pupil information to our local authority and / or providers of youth support services, under the Learning and Skills Act 2000 and the Learning and Skills (Wales) Measure 2009, as they have responsibilities in relation to the education or training; from aged 11 to 19.

This enables them to provide services as follows:

- Youth support services
- Careers advisers
- Post 16 education and training providers

The information shared is limited to the child's name, address and date of birth. However, where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the child / pupil once they reach the age 16 under the Learning and Skills Act 2000 (s.126(2)).

Data is securely transferred to the youth support service and held for in accordance with the Data Protection Act 2018. The receiving organisation e.g. Careers Wales, will then become the Data Controller in respect of the sent information and will provide you with any privacy or fair processing information directly.

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information or be given access to your child's educational record, please contact the school office directly.

In certain circumstances you also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress.
- Prevent processing for the purpose of direct marketing.
- Object to decisions being taken by automated means.
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed.
- A right to seek redress, either through the ICO, or through the courts.

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns

Contact

If you would like to discuss anything in this privacy notice, please contact:
Data Protection Officer:
Alison Matthias,
Creative Learning Room,
Unit 16, Mold Business Park,
Mold
CH7 1XP
Tel: 01352755141

Appendix 2

Seven golden rules for information sharing

1. **Remember that the Data Protection Act is not a barrier to sharing information** but provides a framework to ensure that personal information about living persons is shared appropriately.

2. **Be open and honest** with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement unless it is unsafe or inappropriate to do so.

3. **Seek advice** if you are in any doubt, without disclosing the identity of the person where possible.

4. **Share with consent where appropriate** and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.

5. **Consider safety and well-being.** Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.

6. **Necessary, proportionate, relevant, accurate, timely and secure.** Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up to date, is shared in a timely fashion, and is shared securely.

7. **Keep a record** of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Appendix 3

Subject Access Request Form

This form is designed to help you make the request, however, you do not have to use it

Name of Organisation you are making the request to: Email address of the organisation:

Your name: Your email address: Your telephone number: Proof of ID: *This could be passport or driving licence* Proof of address: *This could be copy of bank statement, utility bill or TV licence*

Please state the subject access request which you are entitled to under Article 15 of the GDPR act

Signature:

Date:

Plesae note, if you are making the request for someone else, you should provide proof of ID and address for them (not for you). You will also need to provide evidence that you're allowed to make the request for them eg a signed letter of consent, a power of attorney document or proof of parental responsibility such as a birth or adoption certificate.

Appendix 4

Data Breach Procedures - Flowchart