General Data Protection Regulation Policy (GDPR)

Contents page

Page 1	Contents Page
Page 2 - 3	**1. Statement of Intent** 1.2 Review 1.3 Legal Framework 1.4 Types of Data
Page 3 - 10	**2. Principles** 2.1 Accountability 2.1.1 Data Protection Officer 2.2 Lawful Processing 2.3 Consent 2.4 The Right to be Informed 2.4 The Right of Access 2.5 The Right to Rectification 2.6 The Right to Erasure 2.7 The Right to Restrict Processing 2.8 The Right to Data Portability 2.9 The Right to Object
Page 10 - 11	3. Automated Decision Making and Profiling 4. Privacy by Design and Privacy Impact Assessments
Page 11	5. Data Breaches
Page 12 -13	6. Data Security 6.1 Paper 6.2 Digital 6.3 Emails 6.4 Keeping Personal Information Secure 6.5 Publication of Information 6.5 CCTV and Photography
Page 13	7. Data Retention
Page 13 -14	8. DBS Data
Page 15 - 21	**Appendix A** Security Breach Prevention and Management Plan
Page 22 - 26	**Appendix B** Photography and Videos at School
	Information Records Management Service Retention Schedule

1. Statement of Intent

1. The Loyne Specialist School and Grizedale Centre is required to keep and process certain information about its pupils, staff, parents or carers and other individuals who come into contact with our establishment. This is in accordance with its legal obligations under the General Data Protection Regulations 2018 (GDPR).
2. The establishment may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's / adult services. Further information can be found in our privacy policies on our website at https://loyneschool.org.uk/policy/
3. This policy is in place to ensure all staff and Governors are aware of their responsibilities and outlines how we comply with the core principles of the GDPR. All staff are involved with, and have responsibility for, the collection, processing and disclosure of personal data and must be aware of their duties and responsibilities by adhering to this policy and the law. Training and refresher training will be delivered to staff to ensure they are aware of their duties under the GDPR.
4. Organisational methods for keeping data secure are imperative. It is good practice to keep clear practical policies that are reviewed and presented to the Governing Body before being shared with staff and made publicly available on our school website where applicable.
5. This policy complies with the requirements set out under the GDPR, which came into effect on 25th May 2018.
6. The nominated **Data Protection Officer (DPO)** is the School Business Manager, **Anna Bradley**, who can be contacted via the main school office on 01524 64543.

1.2 Review

This policy will be reviewed annually, or as and when changes occur.

Signed: (Chair of Governors)

Signed: (Headteacher)

Date: 12/06/2024

Standard Review details

Policy reviewed: April 24
Reviewed by: Anna Bradley
Review date: April 28

1.3 Legal framework

1. This policy has due regard to legislation, including, but not limited to, the following:

    a. The General Data Protection Regulation 2018 (GDPR)
    b. The Freedom of Information Act 2000
    c. The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
    d. The Freedom of Information and Data Protection Regulations 2004
    e. The Data Protection Act 1998
    f. The School Standards and Framework Act 1998

2. This policy will also have regard to the following guidance:

    a. Information Commissioner's Office (ICO) (2017) 'Overview of the General Data Protection Regulation (GDPR)' https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
    b. GDPR Privacy Notices
    c. Lancashire County Council policies relating to the GDPR Data Protection

3. Staff (including Volunteers and Agency Workers) should also refer to the following polices in relation to the GDPR Data Protection:

    a. Child Protection and Safeguarding (including adult safeguarding)
    b. Online Safety
    c. Acceptable Use Policy
    d. Staff Code of Conduct
    e. Staff Handbook
    f. Pupil Privacy Policy
    g. Workforce Privacy Policy
    h. Complaints Policy

1.4 Types of Data

1. For the purpose of this policy, **personal data** refers to information that relates to an identifiable, natural person, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

2. Sensitive personal data is referred to under the GDPR as '**special categories of personal data'**, which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

2. Principles

1. In accordance with the requirements outlined under the GDPR and as detailed in our privacy policies, personal data will be:

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

b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
d. Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that data which is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.
e. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed. Personal / special category data may be stored for longer periods, insofar as the 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.
f. Processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2. The GDPR also requires that the data controller/processor shall be responsible for, and able to demonstrate, compliance with the principles.

2.1 Accountability

1. The Loyne Specialist School and Grizedale Centre will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.
2. We will provide comprehensive, clear and transparent privacy policies which are made publicly available on the website. They are also available on request from the school office.
3. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.
4. Internal records of processing activities will include the following (list not exhaustive):

    a. Name and details of the organisation
    b. Purpose(s) of the processing
    c. Description of the categories of individuals and personal data
    d. Retention schedules
    e. Categories of recipients of personal data
    f. Description of technical and organisational security measures
    g. Details of transfers to other countries, including documentation of the transfer mechanism safeguards in place

5. We will implement measures that meet the principles of data protection by design and data protection by default, such as:

    a. Data minimisation.
    b. Pseudonymisation.
    c. Transparency.

d. Allowing individuals to monitor processing
e. Continuously creating and improving security features.

6. Data protection impact assessments will be used, where appropriate.

2.1.1 Data protection officer (DPO)

The appointed Data Protection Officer is the School Business Manager. With the support of the Senior Leadership team and Governors the DPO has a duty to:

a. Inform and advise employees (including Governors, volunteers and students) about their obligations to comply with the GDPR and other data protection laws.
b. Monitor compliance with the GDPR and other laws, including managing internal data protection activities (as far as possible), advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.
c. The individual appointed as DPO will have some knowledge of data protection law, particularly that in relation to schools, and will seek advice from Legal Services as required.
d. The DPO will report to the highest level of management at the school, which is normally Fthe Headteacher.
e. The DPO will operate independently and will not be dismissed or penalised for performing their task.
f. Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

2.2 Lawful processing

You must have a valid lawful basis in order to process personal data.

There are **six available lawful bases for processing**. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose.

Under the GDPR, data will be lawfully processed under the following conditions:

a. Compliance with a **legal obligation.**
b. **Consent** of the data subject has been obtained unless data processing is necessary as part of the legitimate interests of the business or relates to safeguarding matters and is in the vital interest of the young person/other parties
c. The performance of **a task carried out in the public interest** or in the exercise of official authority vested in the controller.
d. For the **performance of a contract** with the data subject or to take steps to enter into a contract.
e. Protecting the **vital interests** of a data subject or another person.
f. 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. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

4. Personal and special category data will only be processed under the following conditions:

a. Explicit consent of the data subject, unless reliance on consent is prohibited by law.

b. 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.
c. Processing relates to personal data manifestly made public by the data subject.

5. Processing is necessary for:

a. Carrying out obligations under employment, social security or social protection law, or a collective agreement.
b. Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
c. The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
d. Reasons of substantial public interest on the basis of law which is proportionate to the aim pursued and which contains appropriate safeguards.
e. 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.
f. 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.
g. Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

2.3 Consent

1. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
2. Consent can only be given and acted upon by those deemed to have the mental capacity to understand what they are consenting to.
3. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
4. Where consent is given, a record will be kept documenting how and when consent was given. This will be recorded on CPOMS for pupils and in staff folders for staff.
5. The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.
6. Consent accepted under the DPA will be reviewed to ensure it meets the standards of GDPR; however, acceptable consent obtained under the DPA will not be reobtained.
7. Consent can be withdrawn by the individual at any time.
8. Where a child is under the age of 13, or over the age of 13 but does not have mental capacity, the consent of parents / carers will be sought prior to the processing of their data. Consent to process data may not be required in some instances, e.g. the sharing of safeguarding data.
9. If you are relying on consent as your lawful basis for processing, in the UK only children aged 13 or over are able provide their own consent where they are deemed to have the mental capacity to make an informed decision.

2.4 The right to be informed

1. The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.
2. If services are offered directly to a young person or adult with mental capacity, the school / Grizedale Centre will ensure that the privacy notice is written in a clear, plain manner that the young person / adult will understand.
3. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy policy:

    a. The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
    b. The purpose of, and the legal basis for, processing the data.
    c. The legitimate interests of the controller or third party.
    d. Any recipient or categories of recipients of the personal data.
    e. Details of transfers to third countries and the safeguards in place.
    f. The retention period of criteria used to determine the retention period.

4. The existence of the data subject's rights, including the right to:

    a. Withdraw consent at any time.
    b. Lodge a complaint with the named Data Protection Officer in the first instance. In unsatisfied the complainant will need to follow School Complaint Procedures which can be found at www.loyneschool.org.uk/policy
    c. The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

5. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.
6. Where data is not obtained directly from the data subject, information regarding the categories of personal data that the establishment holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.
7. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.
8. In relation to data that is not obtained directly from the data subject, this information will be supplied:
    a. Within one month of having obtained the data.
    b. If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
    c. If the data are used to communicate with the individual, at the latest, when the first communication takes place.

2.5 The right of access

1. Individuals have the right to obtain confirmation that their data is being processed.

2. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.
3. The Data Protection Officer will verify the identity of the person making the request before any information is supplied.
4. A copy of the information will be supplied to the individual free of charge; however, the establishment may impose a 'reasonable fee' to comply with requests for further copies of the same information.
5. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
7. All fees will be based on the administrative cost of providing the information.
8. All requests will be responded to without delay and at the latest, within one month of receipt.
9. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
10. Where a request is manifestly unfounded or excessive, the establishment holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain further following the school's / Grizedale Centre Complaint Procedures within one month of the refusal.
11. In the event that a large quantity of information is being processed about an individual, the DPO will ask the individual to specify the information the request is in relation to.

2.6 The right to rectification

1. Individuals are entitled to have any inaccurate or incomplete personal data rectified.
2. Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.
3. Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.
4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
5. Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

2.7 The right to erasure

1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
2. Individuals have the right to erasure in the following circumstances:

    a. Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
    b. When the individual withdraws their consent
    c. When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
    d. The personal data was unlawfully processed
    e. The personal data is required to be erased in order to comply with a legal obligation
    f. The personal data is processed in relation to the offer of information society services to a child

The school / Grizedale Centre has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

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

3. As a child or young person with SEN who has mental capacity, may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child / young person has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.
4. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.
5. Where personal data has been made public within an online environment, the DPO will inform other organisations who process the personal data to erase links to, and copies of, the personal data in question.

2.8 The right to restrict processing

1. Individuals have the right to block or suppress the establishments processing of personal data.
2. In the event that processing is restricted, the establishment will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.
3. The establishment will restrict the processing of personal data in the following circumstances:

a. Where an individual contests the accuracy of the personal data, processing will be restricted until the DPO has verified the accuracy of the data
b. Where an individual has objected to the processing and the DPO is considering whether their legitimate grounds override those of the individual
c. Where processing is unlawful and the individual opposes erasure and requests restriction instead
d. Where the establishment no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

4. If the personal data in question has been disclosed to third parties, the DPO will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
5. The DPO will inform individuals when a restriction on processing has been lifted.

2.9 The right to data portability

1. Individuals have the right to obtain, and reuse, their personal data for their own purposes across different services.

2. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.
3. The right to data portability only applies in the following cases:

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

4. Personal data will be provided in a structured, commonly used and machine-readable form.
5. The establishment will provide the information free of charge.
6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.
7. The establishment is not required to adopt or maintain processing systems which are technically compatible with other organisations.
8. In the event that the personal data concerns more than one individual, the DPO will consider whether providing the information would prejudice the rights of any other individual.
9. The DPO will respond to any requests for portability within one month.
10. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, provided that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.
11. Where no action is being taken in response to a request, the establishment will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

2.10 The right to object

1. The establishment will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.
2. Individuals have the right to object to the following:

    a. Processing based on legitimate interests or the performance of a task in the public interest
    b. Direct marketing
    c. Processing for purposes of scientific or historical research and statistics.

3. Where personal data is processed for the performance of a legal task or legitimate interests:

    a. An individual's grounds for objecting must relate to his or her particular situation.
    b. The establishment will stop processing the individual's personal data unless the processing is for the school / Grizedale Centre exercise or defence of legal claims, or, where the school / Grizedale Centre can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

4. Where personal data is processed for direct marketing purposes:

a. The DPO will stop processing personal data for direct marketing purposes as soon as an objection is received.
b. The establishment cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

5. Where personal data is processed for research purposes:

a. The individual must have grounds relating to their particular situation in order to exercise their right to object.
b. For the majority of research projects there must be an informed consent process which details the specifics of the research.
c. Where the processing of personal data is necessary for the performance of a public interest task, the school / Grizedale Centre is not required to comply with an objection to the processing of the data.

6. Where the processing activity is outlined above, but is carried out online, the school / Grizedale Centre will offer a method for individuals to object online.

3. Automated decision making and profiling

1. Individuals have the right not to be subject to a decision when:

   a. It is based on automated processing, e.g. profiling.
   b. It produces a legal effect or a similarly significant effect on the individual.

2. The establishment will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.
3. When automatically processing personal data for profiling purposes, the establishment will ensure that the appropriate safeguards are in place, including:
   a. Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
   b. Using appropriate mathematical or statistical procedures.
   c. Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
   d. Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

4. Automated decisions must not concern a child / young adult or be based on the processing of sensitive data, unless:

   a. The school / Grizedale Centre has the explicit consent of the individual (where the individual is deemed to have mental capacity).
   b. The processing is necessary for reasons of substantial public interest on the basis of law.

4. Privacy by design and privacy impact assessments

1. The establishment will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate

2. How the establishment has considered and integrated data protection into processing activities.
3. Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the data protection obligations and meeting individuals' expectations of privacy.
4. DPIAs will allow the establishment to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's / Grizedale Centre reputation which might otherwise occur.
5. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.
6. A DPIA will be used for more than one project, where necessary.
7. High risk processing includes, but is not limited to, the following:
   a. Systematic and extensive processing activities, such as profiling
   b. Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
   c. The use of CCTV.

8. The DPO will ensure that all DPIAs include the following information:

   a. A description of the processing operations and the purposes
   b. An assessment of the necessity and proportionality of the processing in relation to the purpose
   c. An outline of the risks to individuals
   d. The measures implemented in order to address risk

9. Where a DPIA indicates high risk data processing, the DPO or member of the Senior Leadership Team will consult the LA's Legal Services Department and/or the Information Commissioners Office to seek its opinion as to whether the processing operation complies with the GDPR.

5. Data breaches

1. The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
2. The DPO, with the support of the Senior Leadership Team will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their induction and CPD training.
3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.
4. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the establishment becoming aware of it.
5. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

6. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the establishment will notify those concerned directly.
7. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

8. In the event that a breach is sufficiently serious, the public will be notified without undue delay.
9. Effective and robust breach detection, investigation and internal reporting procedures are in place at the school / Grizedale Centre, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.
10. Within a breach notification, the following information will be outlined:

    a. The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
    b. The name and contact details of the DPO
    c. An explanation of the likely consequences of the personal data breach
    d. A description of the proposed measures to be taken to deal with the personal data breach
    e. Where appropriate, a description of the measures taken to mitigate any possible adverse effects

11. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.
12. The Security Breach Prevention and Management Plan is attached at Appendix A.

6. Data security

6.1 Paper

1. Limited paper records relating to learners which may include Behaviour Management Plans, Educational Health Care plans and learner specific information are kept in cupboards in class bases / Grizedale Centre base. Classrooms and the Grizedale Centre are locked by the Site Supervisor when not in use during periods of school closure and before and after the working day once learners and staff have left the building. Visitors during the working day between 8.45 a.m. – 3.15 p.m., including contractors are escorted on the premises. Contractors working during periods of closure access only the areas they need to. Sensitive data is not publicly displayed or easily accessible by anyone other than staff. Learner files are kept in the school office and on our secure network. Grizedale Centre files are held in the Grizedale Centre and on our secure network. Both the office and Grizedale Centre have keypad/swipe access security. Access is restricted to office staff and the senior leadership team, site supervisor and cleaners.
2. Confidential paper records will not be left unattended or in clear view anywhere with general access.

6.2 Digital

1. Digital data is coded, encrypted or password-protected.
2. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use. The device will be encrypted.

3. Memory sticks will not be used to hold personal information unless they are fully encrypted.

4. All electronic devices are password-protected to protect the information on the device in case of theft. Where possible, the establishment enables electronic devices to allow the remote blocking or deletion of data in case of theft.
5. Staff will not store information relating to the school / Grizedale Centre on personal laptops or computers for work purposes.
6. Staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

6.3 Emails

1. Emails containing sensitive or confidential information are encrypted if there are unsecure servers between the sender and the recipient are sent encrypted. This would include any emails that sent to an addresses outside of the authority or Office 365.
2. In the event that an email is sent to a parent, it would be sent from the info@ email address.
3. Where there are multiple email recipients (outside of the school and local authority) emails will be sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
4. When sending confidential information by email, staff will always check that the recipient address is correct before sending.

6.4 Keeping personal information secure

1. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key, ensuring encryption for electronic data etc. The person taking the information from the premises accepts full responsibility for the security of the data.

2. Before sharing data, all staff members will ensure:

    a. They are allowed to share it.
    b. That adequate security is in place to protect it.
    c. Who will receive the data has been outlined in a privacy notice.

3. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school / Grizedale Centre containing sensitive information are supervised at all times.
4. The physical security of the buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
5. The Loyne Specialist School and Grizedale Centre takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
6. The School Business Manager (SBM) and ICT Technician are responsible for ensuring continuity and recovery measures are in place to ensure the security of protected data.

6.5 Publication of information

1. The Loyne Specialist School / Grizedale Centre will not publish any personal information, including photos or videos, on its website or Facebook page without consent from

parents/carers or the young person. Pupil's names will not be used on our website or Facebook page. Our Facebook page is externally and internally monitored and comments or posts that identify pupils by name will be removed.

6.6 CCTV and photography

1. The establishment understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.
2. The establishment does not collect CCTV or share images unless there is a specific reason for doing so. For example, sharing images with the police if there has been an incident of vandalism. Images are automatically overwritten by the CCTV system after 30 days.
3. The establishment will always indicate its intentions for taking photographs/videos of pupils and will obtain permission before publishing them.
4. If the establishment wishes to use images/video footage of pupils in a publication, such as the website, marketing materials or recordings of plays, written permission will be sought for the usage from the parent / carer or the young person if they are over 13 and have mental capacity.
5. Precautions, as outlined in Appendix B 'Use Photography and Videos', are taken when publishing photographs of pupils, in print, video or on the school website.

7. Data retention

1. Data will not be kept for longer than is necessary and in line with the Information Resources Management Service (IRMS) Retention Schedule which is attached to this policy.
2. Unrequired data will be deleted as soon as practicable.
3. Confidential paper documents will be shredded by Lancashire Shredding services who are GDPR compliant. Electronic records will be securely deleted from the network and server once the data should no longer be retained.
4. Staff must check class electronic folders, displays, and other areas in which pupil images may be held and remove them where they are no longer required or contain unlawful data, such as photos where consent has been removed. The IT Technician will take responsibility, in liaison with the DPO, for removing data that is no longer required from the network. This includes archived photos unless there is specific reason to keep them.

8. DBS data

1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.
2. Data provided by the DBS will never be duplicated

3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

APPENDIX A

Security Breach Prevention and Management Plan

A1 Statement of intent

a. The Loyne Specialist School and Grizedale Centre is committed to maintaining the confidentiality of its information and ensuring that the details of the finances, operations, learners and staff are only accessible by the appropriate individuals. It is therefore important to uphold high standards of security, take suitable precautions, and to have systems and procedures in place that support this.

b. The establishment recognises, however, that breaches in security can occur, particularly as the majority of information is stored online or on electronic devices which are increasingly vulnerable to cyber-attacks. This being the case, it is necessary to have a contingency plan containing procedures to minimise the potential negative impacts of any security breach, to alert the relevant authorities, and to take steps to help prevent a repeat occurrence.

c. For the purposes of this policy, the title of 'data controller' will be used in reference to the person(s) primarily responsible for the handling and protection of information and data within a establishment.

A2 Types of security breach and causes

a. Unauthorised use without damage to data – involves unauthorised persons accessing data on our system, e.g. 'hackers', who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it.
b. Unauthorised removal of data – involves an authorised person accessing data, who removes the data to pass it on to another person who is not authorised to view it, e.g. a staff member with authorised access who passes the data on to a friend without authorised access – this is also known as data theft. The data may be forwarded or deleted altogether.
c. Damage to physical systems – involves damage to the hardware in the server/network, which may result in data being inaccessible and/or becoming accessible to unauthorised persons.
d. Unauthorised damage to data – involves an unauthorised person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.
e. Breaches in security may be caused as a result of actions by individuals, which may be accidental, malicious or the result of negligence – these can include:
f. Accidental breaches, e.g. as a result of insufficient training for staff, so they are unaware of the procedures to follow.
g. Malicious breaches, e.g. as a result of a hacker wishing to cause damage to the establishment through accessing and altering, sharing or removing data.
h. Negligence, e.g. as a result of an employee that is aware of school / Grizedale Centre policies and procedures, but disregards these.
i. Breaches in security may also be caused as a result of system issues, which could involve incorrect installation, configuration problems or an operational error – these can include:
    - Incorrect installation of anti-virus software and/or use of software which is not the most up-to-date version, meaning that software is more vulnerable to a virus;
    - Incorrect firewall settings are applied, e.g. access to the network, meaning individuals other than those required could access the system;

- Confusion between backup copies of data, meaning the most recent data could be overwritten.

A3 Roles and responsibilities

a. The SBM/DPO and ICT Technician are responsible for implementing effective strategies for the management of risks posed by internet use, and to keep its network services, data and users secure.
b. The Data Protection Officer (DPO) is responsible for the overall monitoring and management of data security.
c. The SBM/DPO is responsible for establishing a procedure for managing and logging incidents.
d. The Governing Body is responsible for holding regular meetings with the Headteacher and Data Protection Officer to discuss the effectiveness of data security, and to review incident logs.
e. All members of staff and learners are responsible for adhering to the processes outlined in the relevant policies as detailed.

A4 Secure configuration

a. An inventory will be kept of all IT hardware and software currently in use, including personal devices provided by the establishment to staff. This will be stored on the network and will be audited on a termly basis by the IT Technician to ensure it is up-to-date.
b. Any changes to the IT hardware or software will be documented using the inventory, and will be authorised by the data controller before use.
c. All systems will be audited on a termly basis to ensure the software is up-to-date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security, and will be recorded on the inventory.
d. Any software that is out-of-date or reaches its 'end of life' will be removed from systems, i.e. when suppliers end their support for outdated products such that any security issues will not be rectified.
e. All hardware, software and operating systems will require passwords for individual users before use. Passwords will be changed on a termly basis to prevent access to facilities which could compromise network security.
f. The establishment believes that locking down hardware, such as through the use of strong passwords, is an effective way to prevent access to facilities by unauthorised users.

A5 Network security

a. The establishment will employ firewalls in order to prevent unauthorised access to the systems. The firewall will be deployed as a centralised deployment: the broadband service connects to a firewall that is located within a data centre or other major network location.
b. Any compromise of security through the firewall is recorded by the SBM/DPO using an incident log and is reported to the Headteacher. The SBM/DPO and ICT Technician will react to security threats to find new ways of managing the firewall.

A6 Malware prevention

a. The establishment understands that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media controls.
b. The IT technician will ensure that all devices owned by the establishment have secure malware protection and undergo regular malware scans.

c. The IT co-ordinator will update malware protection on a termly basis to ensure it is up-to-date and can react to changing threats.
d. Malware protection will also be updated in the event of any attacks to the establishments hardware and software.
e. Filtering of websites, as detailed in sections A7d and A9 of this policy, will ensure that access to websites with known malware is blocked immediately and reported to the DPO.
f. The establishment will use mail security technology, which will detect and block any malware that is transmitted by email. This will also detect any spam or other messages which are designed to exploit users.
g. The IT co-ordinator will review the mail security technology on an annual basis to ensure it is kept up-to-date and effective.

A7 User privileges

a. The establishment understands that controlling what users have access to is important for promoting network security. User privileges will be differentiated, i.e. pupils will have different access to data and the network than members of staff.
b. The ICT Technician will clearly define what users have access to and will communicate this to the data controller.
c. The ICT Technician will ensure that user accounts are set up to allow users access to the facilities required whilst minimising the potential for deliberate or accidental attacks on the network.
d. The ICT Technician will ensure that websites are filtered for inappropriate and malicious content. Any member of staff or pupil that has accessed inappropriate or malicious content will be recorded in accordance with the monitoring process in section A8 of this policy.
e. All users must set passwords are strong and contain a mixture of letters, numbers, lower and higher case, symbols etc. Users will also be required to change their password if they become known to other individuals. Pupils are responsible for remembering their passwords; however, the ICT Technician will have an up-to-date record of all usernames and passwords, and will be able to reset them if necessary.
f. The 'master user' password used by the ICT Technician will be made available to the DPO on request if required.
g. Automated user provisioning systems will be employed in order to automatically delete inactive users or users who have left. The ICT Technician will manage this provision to ensure that all users that should be deleted are, and that they do not have access to the system.
h. The ICT Technician will review the system on a termly basis to ensure the system is working at the required level.

A8 Monitoring usage

a. Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by pupils or staff.
b. The Senior Leadership Team will inform all learners and staff that their usage will be monitored, in accordance with the Acceptable Use Policy and Online Safety Policy.
c. If a user accesses inappropriate content or a threat is detected, an alert will be sent to the ICT Technician. Alerts will also be sent for unauthorised and accidental usage.
d. Alerts will identify: the user, the activity that prompted the alert and the information or service the user was attempting to access.
e. The DPO will record any alerts using an incident log and will report this to the Headteacher. All incidents will be responded to in accordance with this policy, and as outlined in the Online Safety policy.

A9 Removable media controls and home working

a. The establishment understands that staff may need to access the network from areas other than on the premises. Effective security management will be established to prevent access to, or leakage of, data, as well as any possible risk of malware.
b. The ICT Technician will encrypt all establishment-owned devices for personal use, such as laptops, and tablets, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data. USB sticks must **NOT** be used unless they are encrypted. Staff must liaise with the DPO or IT Technician if they require an encrypted pen drive.
c. When using laptops, tablets and other portable devices, the ICT Technician will determine the limitations for access to the network, as described in section A7 user privileges of this policy.
d. Staff who use establishment-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off the premises.
e. The ICT Technician will use encryption to filter the use of websites on these devices, in order to prevent inappropriate use and external threats which may compromise network security when bringing the device back onto the premises.
f. The establishment uses tracking technology where possible to ensure that lost or stolen devices can be retrieved. All ICT equipment will be asset tagged over the summer period 2018.
g. All data will be held on systems centrally in order to reduce the need for the creation of multiple copies, and/or the need to transfer data using removable media controls.
h. The Wi-Fi network will be password protected and will only be given out as required. Staff and pupils are not permitted to use the Wi-Fi for their personal devices, such as mobile phones or tablets.
i. A separate Wi-Fi network will be established for visitors to limit their access to printers, shared storage areas and any other applications which are not necessary.

A10 Backing-up data

a. Back-ups are run overnight and are completed before the beginning of the next day.
b. Upon completion of back-ups, data is stored externally by the Lancashire County Council.
c. Only authorised personnel are able to access school / Grizedale Centre data.

A11 User training and awareness

a. Training for all staff members will be arranged by the Data Protection Officer within two weeks following an attack or significant update.
b. Through training, all staff will be aware of who they should inform first in the event that they suspect a security breach, and who they should inform if they suspect someone else is using their passwords.
c. All staff will receive the GDPR policy as part of their induction programme.
d. All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks, in accordance with the process detailed in the Acceptable Use Policy and Staff Code of Conduct.

A12 Security breach incidents

a. Any individual that discovers a security data breach will report this immediately to the Data Protection Officer. When an incident is raised, the DPO will record the following information:

- Name of the individual who has raised the incident
- Description of the incident
- Description of any perceived impact
- Description and identification codes of any devices involved e.g. establishment-owned laptop
- Location of the equipment involved
- Contact details for the individual who discovered the incident

b. The DPO will take the lead in investigating the breach, and will be allocated the appropriate time and resources to conduct this. The DPO, as quickly as reasonably possible, will ascertain the severity of the breach and determine if any personal data is involved or compromised. The DPO will oversee a full investigation and produce a comprehensive report. The cause of the breach, and whether or not it has been contained, will be identified – ensuring that the possibility of further loss/jeopardising of data is eliminated or restricted as much as possible.

c. If the DPO determines that the severity of the security breach is low, the incident will be managed in accordance with the following procedures:
   - In the event of an internal breach, the incident is recorded using an incident log, and by identifying the user and the website or service they were trying to access.
   - The Headteacher will issue disciplinary sanctions to the pupil or member of staff, in accordance with the relevant policies.
   - The DPO will work with the third-party provider to provide an appropriate response to the attack, including any in-house changes. Any further action which could be taken to recover lost or damaged data will be identified – this includes the physical recovery of data, as well as the use of back-ups.

d. Where the security risk is high, the DPO will establish what steps need to be taken to prevent further data loss which will require support from various departments and staff. This action may include:

   - Informing the ICO
   - Informing relevant staff of their roles and responsibilities in areas of the containment process.
   - Taking systems offline.
   - Retrieving any lost, stolen or otherwise unaccounted for data.
   - Restricting access to systems entirely or to a small group.
   - Backing up all existing data and storing it in a safe location.
   - Reviewing basic security, including:
   - Changing passwords and login details on electronic equipment.
   - Ensuring access to places where electronic or hard data is kept is monitored and requires authorisation.

e. Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the DPO will inform the police of the security breach. The ICT Technician will test all systems to ensure they are functioning normally, and the incident will only be deemed ‘resolved’ when it has been assured that the systems are safe to use.

A13 Assessment of risks

a. The following questions will be considered by the Data Protection Officer in order to fully and effectively assess the risks that the security breach has brought, and to help take the next appropriate steps. All relevant questions will be clearly and fully answered in the Data Protection Officer’s report and records:

I) What type and how much data is involved?
II) How sensitive is the data?
- Sensitive data is defined in the Data Protection Act 1998; some data is sensitive because of its very personal nature (e.g. health records) while other data types are sensitive because of what might happen if it is misused (e.g. bank account details).

iii) Is it possible to identify what has happened to the data – has it been lost, stolen, deleted or tampered with?
- If the data has been lost or stolen, were there any protective measures in place to prevent this, such as data and device encryption?

iv) If the data has been compromised, have there been effective measures in place that have mitigated the impact of this, such as the creation of back-up tapes and spare copies?
v) Has individuals' personal data been compromised – how many individuals are affected?
vi) Who are these individuals – are they pupils, staff, governors, volunteers, stakeholders, suppliers?
vii) Could their information be misused or manipulated in any way?
viii) Could harm come to individuals? This could include risks to the following:
- Physical safety
- Emotional wellbeing
- Reputation
- Finances
- Identity
- Private affairs becoming public

ix) Are there further implications beyond the risks to individuals? Is there a risk of loss of public confidence/damage to the school's reputation, or risk to the school's operations?
x) Who could help or advise the school on the breach? Could the LA, external partners, authorities, or others provide effective support?

b. In the event that the DPO, or other persons involved in assessing the risks to the school, are not confident in the risk assessment, they will seek advice from the Information Commissioner's Office (ICO).

A14 Consideration of further notification

a. The DPO in liaison with the Senior Leadership Team, will consider whether there are any legal, contractual or regulatory requirements to notify individuals or organisations that may be affected or who will have an interest in security.
b. The DPO in liaison with the Senior Leadership Team, will decide whether notification will help the establishment meet its security obligations under the seventh data protection principle.
c. The DPO in liaison with the Senior Leadership Team, will assess whether notification could help the individual(s) affected, and whether individuals could act on the information provided to mitigate risks, e.g. by cancelling a credit card or changing a password.
d. If a large number of people are affected, or there are very serious consequences, the ICO will be informed.
e. The DPO in liaison with the Senior Leadership Team, will consider who to notify, what to tell them and how they will communicate the message, which may include:

i) A description of how and when the breach occurred and what data was involved. Details of what has already been done to respond to the risks posed by the breach will be included.
ii) Specific and clear advice on the steps they can take to protect themselves, and what the establishment is willing to do to help them.
iii) A way in which they can contact the school /Grizedale Centre for further information or to ask questions about what has occurred.
iv) The DPO in liaison with the Senior Leadership Team, will consult the ICO for guidance on when and how to notify them about breaches. The DPO in liaison with the Senior Leadership Team, will consider, as necessary, the need to notify any third parties – police, insurers, professional bodies, funders, trade unions, website/system owners, banks/credit card companies – who can assist in helping or mitigating the impact on individuals.

4. Under the GDPR, the following steps will be taken if a breach of personal data occurs:

I. The DPO in liaison with the Senior Leadership Team, will notify the ICO within 72 hours of a breach where it is likely to result in a risk to the rights and freedoms of individuals.
II. Where a breach is likely to result in significant risk to the rights and freedoms of individuals, the DPO in liaison with the Senior Leadership Team, will notify those concerned directly with the breach.

Where the breach compromises personal information, the notification will contain:

III. The nature of the personal data breach including, where possible:

a) The type(s), e.g. staff, learners, or Governors, and approximate number of individuals concerned.
b) The type(s) and approximate number of personal data records concerned. The name and contact details of the DPO or other person(s) responsible for handling the information.
c) A description of the likely consequences of the personal data breach.
d) A description of the measures taken, or proposed, to deal with and contain the breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

A15 Evaluation and response

1. The DPO in liaison with the Senior Leadership Team, will establish the root of the breach, and where any present or future risks lie.
2. The DPO in liaison with the Senior Leadership Team, will consider the data and contexts involved.
3. The DPO in liaison with the Senior Leadership Team, will identify any weak points in existing security measures and procedures.
4. The DPO in liaison with the Senior Leadership Team, will identify any weak points in levels of security awareness and training.
5. The DPO in liaison with the Senior Leadership Team, will report on findings and, with the approval of the school leadership team, implement the recommendations of the report after analysis and discussion.

Sample Incident Log Form:

Timeline of Incident Management

Date	Time	Activity	Decision	Name/position	Date

APPENDIX B

Photography and Videos

B1 Statement of intent

1. At The Loyne Specialist School and Grizedale Centre we use imagery and videos for a variety of purposes, for example, on communication aids, display boards, resources for educational purposes, the website and Facebook page (list not exhaustive). Whilst we understand that parents/carers may wish to take videos or photos of their children participating in events on or offsite, unfortunately The Loyne Specialist School and Grizedale Centre does not permit the taking of photos or recording of videos of our learners. This is to safeguard our learners.
2. Whilst the GDPR is not applicable to images captured for personal use, we believe that the safeguarding of all learners is paramount at all times. In allowing the recording and taking of images by parents/carers/family the establishment does not have control over where these images may end up. Imagery of learners who do not have permission to appear publicly, particularly on social media, may inadvertently be captured in the background which may result in a complaint. We therefore request that parents/carers respect the our decision to not allow the use of smart phone/cameras/smart watches whilst on site, unless explicit permission has been granted by the Headteacher.

Images taken and used by the Establishment

3. Whilst we recognise the benefits of photography and videos to our community, we also understand that these can have significant risks for those involved. Under the legal obligations of the GDPR, the establishment has specific responsibilities in terms of how photos and videos are taken, stored and retained.
4. The school and Grizedale Centre has implemented a policy on the safe use of cameras and videos by staff which reflect our safeguarding measures.
5. In order to ensure that, as far as possible, the use of photography and video is used safely at all times, the policy provided below should be followed. This policy is applicable to all forms of visual media, including film, print, video, DVD and websites.

Definitions

6. For the purpose of this policy:

    a. **"Personal use"** of photography and videos is defined as the use of cameras/smart phones/watches to take images and recordings of learners by relatives, friends or known individuals, e.g. a parent taking a group photo of their child and their friends at a school event. The principles of the GDPR do not apply to images and videos taken for personal use. However, for the reasons as outlined above The Loyne Specialist School and Grizedale Centre does not allow parents/carers/families etc to record or take images of learners.
    b. **"Official use"** is defined as photography and videos which are used for school / Grizedale Centre purposes, e.g., resources, displays, communication aids. These images are likely to be stored electronically alongside other personal data. The principles of the GDPR apply to images and videos taken for official use.
    c. **"Media use"** is defined as photography and videos which are intended for a wide audience, e.g. photographs of learners taken for a local newspaper, our website and Facebook page. The principles of the GDPR apply to images and videos taken for media use.
    d. Staff may also take photos and videos of ~~pupils~~ learners for **"educational / developmental purposes"** which may be used for a variety of reasons, such as

displays, special events, assessment and workbooks. The principles of the GDPR apply to images and videos taken for educational purposes.

B2 Roles and responsibilities

The Office staff are responsible for:

1. Liaising with social workers/carers to gain consent for photography and videos of Looked After Children (LAC).
2. Liaising with the DPO, to ensure there are no data protection breaches.
3. Informing relevant bodies of any known changes to a learners security, e.g. child protection concerns, which would mean that participating in photography and video recordings would put them at significant risk.

It is the responsibility of all staff:

4. To ensure that all photos and videos are stored and disposed of correctly, in line with the GDPR.
5. Communicating this policy to all the relevant staff members and the wider community, such as parents/carers.

Parents/ Carers are responsible for:

6. Completing the Data Collection Form.
7. Informing the school / Grizedale Centre in writing where there are any changes to their consent.
8. Acting in accordance with this policy.

the DPO is responsible for:

9. Informing and advising employees about their obligations to comply with the GDPR in relation to photographs and videos.
10. Monitoring compliance with the GDPR in regards to processing photographs and videos.
11. Advising on DPIA's in relation to photographs and videos.
12. Conducting internal audits, in regards to procedures for obtaining, processing and using photographs and videos.
13. Providing the required training to staff members, in relation to how the GDPR impacts photographs and videos.

B3 Parental consent

1. The establishment understands that consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
3. Where consent is given, a record will be kept documenting how and when consent was given and last updated.
4. The establishment ensures that consent mechanisms meet the standards of GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data will be found, or the processing will cease.
5. The consent of parents/carers will be sought prior to the processing of data for all our learners, except where the processing is related to preventative or counselling services offered directly to a child over the age of 13. Children over the age of 13 and young adults, where they have mental capacity, may give consent for the processing of their personal data.
6. If the law provides it, children as young as 13 may be permitted to provide consent to the processing of their data.

7. All parents will be asked to update the Data Collection Form on an annual basis, which will determine whether or not they allow their child to participate in photographs and videos.
8. The Data Collection Form will be valid for the full academic year, unless circumstances change in any way, e.g. consent is withdrawn. Additional consent forms will be required if circumstances change.
9. If there is a disagreement over consent, or if a parent does not respond to a consent request, it will be treated as if consent has **not been given**, and photographs and videos will not be taken or published of the learner whose parents have not consented.
10. All parents / carers are entitled to withdraw or change their consent at any time.
11. Parents / carers will be required to confirm on the Data Collection Form, in writing, that they will notify the establishment if their circumstances change in any way, or if they wish to withdraw their consent.
12. For any Looked After Children (LAC) pupils, or pupils who are adopted, the Designated Teacher for LAC will liaise with the pupil's social worker, carers or adoptive parents to establish where consent should be sought. Consideration will be given as to whether identification of an LAC pupil, or pupils who are adopted, would risk their security in any way.
13. Consideration will also be given to any pupils for whom child protection concerns have been raised. Should the Designated Safeguarding Lead (DSL) believe that taking photographs and videos of any pupils would put their security at further risk, greater care will be taken towards protecting their identity.
14. A list of all the names of learners for whom consent was not given will be created by the School Office and will be circulated to all staff members. This list will be updated as changes occur and information circulated to all staff via email.
15. If any parent withdraws or changes their consent, or the DSL reports any changes to a pupil's security risk, or there are any other changes to consent, the list will also be updated and re-circulated.

B4 General procedures

1. Photographs and videos of learners will be carefully planned before any activity.
2. Where photographs and videos will involve LAC pupils, adopted pupils, or pupils for whom there are security concerns, the Headteacher will determine the steps involved.
3. When organising photography and videos of pupils, staff are asked to consider the following:

    a. Can general shots of classrooms or group activities, rather than individual shots of pupils, be used to fulfil the same purpose?
    b. Could the camera angle be amended in any way to avoid pupils being identified?
    c. Will pupils be suitably dressed to be photographed and videoed?
    d. Will pupils of different ethnic backgrounds and abilities be included within the photographs or videos to support diversity?
    e. Would it be appropriate to edit the photos or videos in any way? E.g. to remove logos which may identify pupils?
    f. Are the photographs and videos of the pupils completely necessary, or could alternative methods be used for the same purpose? E.g. could an article be illustrated by pupils' work rather than images or videos of the pupils themselves?
    g. The list of all pupils of whom photographs and videos must not be taken will be checked prior to the activity. Only learners for whom consent has been given will be able to participate.
    h. Images of learners must NEVER be taken on personal devices.

i. Where possible, staff will avoid identifying pupils. If names are required, only first names will be used.
j. The establishment will not use images or footage of any learner who is subject to a court order.
k. The establishment will not use photographs of learners or staff members who have left the school, without consent.
l. Photos and videos that may cause any distress, upset or embarrassment will not be used.
m. Any concern relating to inappropriate or intrusive photography or publication of content is to be reported to the DPO.

B5 Additional safeguarding procedures

1. The establishment understands that certain circumstances may put a pupil's security at greater risk and, thus, may mean extra precautions are required to protect their identity.
2. Any additional measures required will be determined between the DSL, social worker, parents/carers and DPO with a view to minimise any impact on the pupil's day-to-day life.

B6 Establishment owned devices

1. Staff are permitted to take photos and videos of learners using establishment owned equipment only.
2. Where establishment-owned devices are used, images and videos will be saved to the network at the earliest opportunity and removed from the device.
3. Staff will not use their personal mobile phones, or any other personal device, to take images and videos of pupils.
4. Photographs and videos taken by staff members on visits may be used for educational purposes, e.g. on displays or to illustrate the work of the school / Grizedale Centre, where consent has been obtained.
5. Digital photographs and videos held on the network are accessible to staff only. Photographs and videos are stored in labelled files, annotated with the date, and are only identifiable by year group/class number – no names are associated with images and videos. Files are password protected, and only staff members have access to these passwords – these are updated termly to minimise the risk of access by unauthorised individuals.

B7 Use of a professional photographer

1. If the establishment decides to use a professional photographer for official school photos events or marketing, the Headteacher will:

    a. Provide a clear brief for the photographer about what is considered appropriate, in terms of both content and behaviour.

2. The **Office staff** will:

    a. Issue the photographer with identification, which must be worn at all times.
    b. Let learners and parents know that a photographer will be in attendance at an event and ensure they have previously provided consent to both the taking and publication of videos or photographs.
    c. Not allow unsupervised access to pupils or one-to-one photo sessions at events.
    d. Communicate to the photographer that the material may only be used for the school's / Grizedale Centres's own purposes and that permission has not been given to use the photographs for any other purpose.
    e. Ensure that the photographer will comply with the requirements set out in GDPR.

B8 Storage and retention

3. Images obtained by the establishment will not be kept for longer than necessary.
4. Hard copies of photos and video recordings held by the establishment will be annotated with the date on which they were taken and will be stored securely. They will not be used other than for their original purpose, unless permission is sought from the Headteacher and parents of the pupils involved and the DPO has been consulted.
5. Paper documents will be shredded by Lancashire Shredding Services, and electronic records will be securely removed from the network and server once the data should no longer be retained.
6. The ICT Technician will review stored images and videos on an annual basis to ensure that all unwanted material has been deleted.
7. Parents/carers must inform the school / Grizedale Centre in writing where they wish to withdraw or change their consent. If they do so, any related imagery and videos involving their child will be removed from public view.
8. When a parent/carer withdraws consent, it will not affect the use of any images or videos for which consent had already been obtained. Withdrawal of consent will only affect further processing.
9. Official school photos are held on SIMS alongside other personal information, and are retained for the length of the pupil's attendance at the school, or longer, if necessary.

9. References

- https://ico.org.uk/
- https://www.gov.uk/government/publications/data-protection-toolkit-for-schools
- https://www.theschoolbus.net/home
- https://schoolsportal.lancsngfl.ac.uk/sp_atoz/service.asp?u_id=2121&strSL=L
- http://www.actnow.org.uk/content/227

10. Further reading

- An Overview of the General Data Protection Regulation https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-13.pdf
- Guide to the General Data Protection Act https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- A Practical Guide to IT Security https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf
- Subject Access Code of Practice https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf
- A Data Protection Code for Practice Surveillance Cameras and Personal Information https://ico.org.uk/media/1542/cctv-code-of-practice.pdf