Durham Johnston

GDPR / DATA PROTECTION POLICY

1	**SUMMARY**	The aim of this policy is to provide a framework to enable staff, parents and pupils to understand: the law regarding personal data; how personal data should be processed, stored, archived and disposed of and the rights in respect of people whose data is being held and processed by the school, (this includes pupils, parents, staff and governors).			
2	**RESPONSIBLE PERSON:**	Data Protection Officer (DPO) / Headteacher			
3	**APPLIES TO:**	All DJCS Employees			
4	**GROUPS/ INDIVIDUALS WHO HAVE OVERSEEN THE DEVELOPMENT OF THIS POLICY:**	GDPR Team / DPO			
5	**RATIFYING COMMITTEE(S) & DATE OF FINAL APPROVAL:**	FGP & HR Sub-Committee 4 July 2019			
6	**VERSION:**	4.0			
7	**AVAILABLE ON:**	**Staff Shared Drive**	Yes	**Website**	Yes
8	**RELATED DOCUMENTS:**	ICT Policy / Privacy Notices / Retention Policy			
9	**DISSEMINATED TO:**	All DJCS staff including agency / supply staff			
10	**DATE OF IMPLEMENTATION:**	May 2019			
11	**DATE OF NEXT FORMAL REVIEW:**	July 2020			

Date	Version	Action	Amendments
May 2018	1.0	Policy first implemented	N/A
February 2019	2.0	Policy amended	Updates made to Section 11 Subject Access Requests in order to comply with new National Guidance
May 2019	3.0	Policy amended	Whole policy reviewed and updated to comply with regulations
October 2019	4.0	Policy amended	GDPR Team Flowchart updated due to reflect change of the DPO and School LG – GDPR Lead

CONTENTS

1. AIMS & OBJECTIVES

The aim of this policy is to provide a framework to enable staff, parents and pupils to understand:

- the law regarding personal data
- how personal data should be processed, stored, archived and disposed of
- the rights in respect of people whose data is being held and processed by the school (this includes pupils, parents, staff, governors and visitors).

1.1 Safeguarding

The Data Protection Act 2018 and GDPR do not prevent, or limit, the sharing of information for the purposes of keeping children safe. Fears about sharing information will not be allowed to stand in the way of the need to promote the welfare and protect the safety of children.
Keeping children safe in Education
https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

1.2 It is a statutory requirement for all schools to have a Data Protection Policy:

(http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/a00201669/statutory policies-for-schools)

In addition to this policy, schools should have:

- **Retention Information** - details on how long all records are retained
- **Information Asset Audit** - a comprehensive audit listing all the information that the school holds, who has access to the information and the legal basis for processing it
- **Privacy Notices -** for pupils, parents, staff, governors and visitors
- **Registered with the ICO**

This policy will link with the following:

- Safeguarding Policy
- Staff AUP/Code of Conduct
- School Photography Code of Practice
- Photographic Consent Forms

1.3 Definitions

- Personal Data - information relating to a living individual, who can be identified directly from that data or indirectly by reference to other data held. (Note that information can be in any form - written, on a PC e.g. names, addresses, photos.)
- Data Processor – a person who handles the data including filing or storing it.
- Data Subject – the person about whom personal data is processed or kept.
- Data Controller - the person or organisation who determines the "how and what" of data processing in an organisation.

1.4 Data Protection Principles

Article 5 (1) of the GDPR sets out that personal data shall 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; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, not be considered to be incompatible with the initial 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 personal data that are inaccurate, having regard to the purposes for which they are processed, are 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 personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals,

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

In addition, article 5(2) requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles. In effect the school, as the 'data controller', MUST be able to show that its policies and systems comply with requirements of GDPR.

2. LAWFUL BASIS FOR PROCESSING DATA

GDPR stipulates that there must be a lawful basis for processing data and that, for special category data, an additional condition is met. The vast majority of information that the school collects and processes is required to enable the school to perform tasks carried out in the public interest or in the exercise of official authority vested in the school, as the data controller. This is the main lawful basis for processing data that the school relies on.

In addition, there are other bases, such as specific legal obligation applying to the school, as the data controller, that makes the processing necessary.

2.1 Age

Pupils under the age of 13 are not usually considered able to give consent to process their data or to directly access the rights of a data subject, so, parents or guardians can do this on their behalf, providing this is in the best interests of the child. See https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-rights-do-children-have/

Children will be provided with age appropriate advice about how their data is used.

2.2 Consent

If there is a lawful basis for collecting data then consent to collect data is not required (an employee could not opt to withhold an NI number for example). However, a privacy notice, which explains to data subjects (or the parents of the data subject) is required. This explains the lawful basis for processing the data, and also explains to the individual their rights.

Parents/Carers or age appropriate pupils are approached and asked to give consent when there is not a legal reason for processing. This may apply, for instance, for images used in school publicity or social media feeds. The school will ensure that the consent is transparent, revocable, and gathered on an "Opt-in" basis.

3. RIGHTS

The GDPR creates some new rights for individuals and strengthens some existing ones. It provides for the following rights:

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

Different rights are attached to different lawful bases of processing:

	Right to erasure	**Right to portability**	**Right to object**
Vital Interests	✓	**X**	**X**
Legal Obligation	X	**X**	**X**
Public Task	**X**	**X**	✓
Legitimate Interests	✓	**X**	✓
Contract	✓	✓	**X**
Consent	✓	✓	X but right to withdraw consent

3.1 The right to be informed

3.2 The right of access

Depending on the age of the pupil, there are two legal basis for pupils or parents to request access to their data – a Subject Access Request or a request under the 2005 Education Regulations.

3.2.1 Subject Access request under GDPR – please refer to Section 11 of this Policy

GDPR gives individuals the right to access any data that an organisation holds on them. Normally this has to be provided within 30 days without charge. Further guidance is available

at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/
Schools should be aware that guidance from the ICO highlights the rights of the child. *"Before responding to a subject access request for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then you should usually respond directly to the child. You may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child."*

3.2.2 In maintained schools, parents have another statutory right to access their children's educational record

This is part of the Education (Pupil Information) Regulations 2005. This applies to all children under 16 years and has to be provided in 15 working days.
See https://ico.org.uk/your-data-matters/schools/pupils-info/

3.2.3 Information which may be withheld

On some occasions records could contain information which ***"is likely to cause significant harm to the physical or mental health of the child or others",*** for instance, if a child makes a disclosure of abuse. In these circumstances, the data will not be released and the pupil/parent does not need to be informed of its existence. If in doubt, the school will seek legal advice.

3.3 The right to erasure

GDPR includes a right to erasure. However, this is not an absolute right and does not necessarily override the lawful basis for continuing to hold data. Schools' data management systems such as SIMS will begin to improve their functionality to either delete or anonymise personal data when appropriate.

It will be seen from the table above that where a school relies on either a 'legal obligation' or a 'public task' basis for processing (see above) there is no right to erasure. However, this does not mean the data will never be erased. It will still not be retained for any longer than necessary, in accordance with statutory requirements and/or the school's data retention guidelines.

4. DATA TYPES

Not all data needs to be protected to the same standards - the more sensitive or potentially damaging the loss of the data is, the better it needs to be secured. There is, inevitably, a compromise between usability of systems and working with data. In a school environment staff are used to managing risk, for instance during a PE or cooking lesson where risks are assessed, controlled and managed. A similar process takes place with managing school data. GDPR defines different types of data and prescribes how it should be treated.

The loss or theft of any Personal Data is a "Potential Data Breach" which can result in legal action against the school. The loss of sensitive, or "special category", personal data is considered much more seriously and the sanctions may well be more punitive.

4.1 Personal data

The school will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils / students, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, disciplinary records
- Curricular / academic data e.g. class lists, pupil / student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records, disciplinary records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

4.2 Special Category Data

"Special Category Data" are data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning a person's health or sexual life is prohibited except in special circumstances.

This is because special category data is more sensitive and so needs more protection.

In our school the most likely special category data is:

- information on the racial or ethnic origin of a pupil or member of staff
- information about the sexuality of a pupil, his or her family or a member of staff
- medical information about a pupil or member of staff (SEND)
  (Some information regarding safeguarding will also fall into this category)
- staffing e.g. Staff Trade Union membership details

Note – See section on sharing information.

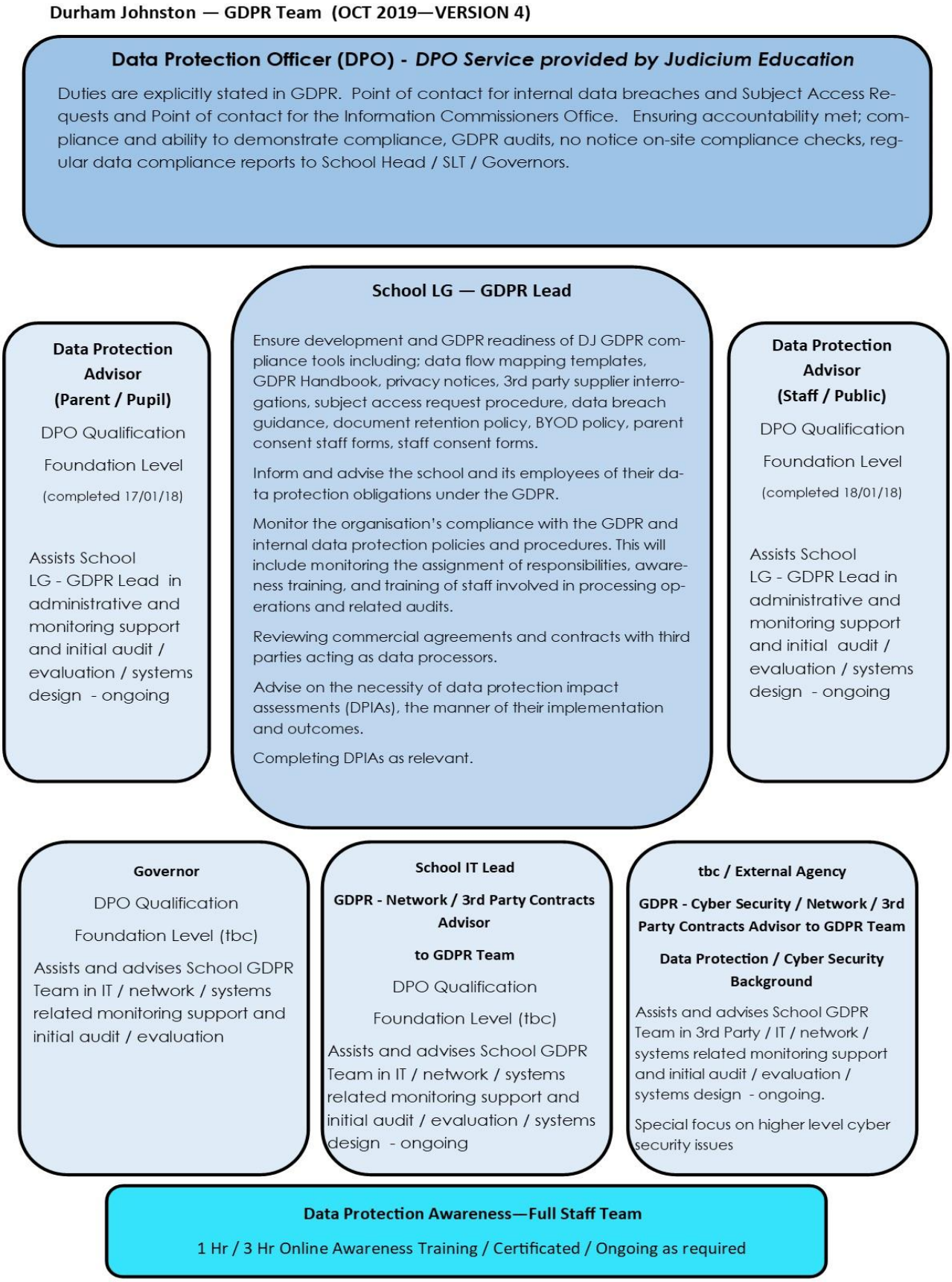
4.3 Other types of Data not covered by the act

This is data that does not identify a living individual and, therefore, is not covered by the remit of the GDPR - this may fall under other 'access to information' procedures. This would include Lesson Plans (where no individual pupil is named), Teaching Resources, and other information about the school, which does not relate to an individual. Some of this data would be available publicly (for instance the diary for the forthcoming year), and some of this may need to be protected by the school (if the school has written a detailed scheme of work that it wishes to sell to other schools).

Schools may choose to protect some data in this category but there is no legal requirement to do so.

5. ROLES & RESPONSIBILITIES

The Headteacher and Governing Body are responsible for Data Protection. The arrangements and roles in place for managing Data Protection at Durham Johnston School, with clear lines of responsibility, are shown here;



5.1 Risk management - Staff and Governors Responsibilities

- Every staff member in the school has responsibility for handling personal information in a safe and secure manner and in accordance with GDPR.
- Governors are also required to comply fully with this policy, in the event that they have access to personal data, when engaged in their role as a Governor.

6. LEGAL REQUIREMENTS

6.1 Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

6.2 Information for Data Subjects (Parents, Carers, Pupils, Younger Pupils, Visitors, Governors and Staff): PRIVACY NOTICES

In order to comply with the fair processing requirements for Data Protection, the school **must** inform parents / carers of all pupils / students, Governors, visitors and staff of the data they collect, process and hold, the purposes for which the data is held, the legal basis for holding it and the third parties (e.g. LA, DfE, etc.) with whom it may be shared.

This information is contained in the school's Privacy Notices, which also set out the data subjects' rights under the GDPR.

New privacy notices were issued to all 'data subjects' by May 2018 even if the data subject had previously received a similar notice. This is because of the new rights in the GDPR that people needed to be informed about. Privacy notices are made available to pupils, parents, carers, Governors, staff and visitors, by publishing on the school website and a paper copy is made available when pupils first register for school.

Pupils are provided with age appropriate information about how their data is being used.

7. TRANSPORTING, STORING AND DISPOSING OF PERSONAL DATA

7.1 Information security - Storage and Access to Data

Clearly, the more sensitive the data the more robust the security measures will need to be in place to protect it. Please refer to the school's ICT Policy.

7.1.1 Technical Requirements

The school has a robust and detailed ICT Policy, which clearly sets out staff and pupil responsibilities and requirements in relation to network acceptable use, end user authentication, internet acceptable use, IT related safeguarding, data storage, mobile data storage, data sharing and use of social media.

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files

are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media will be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data will only be stored on school equipment (this includes computers and portable storage media (provided by the school and encrypted prior to issue). Private equipment (i.e. owned by the users) will not be used for the storage of personal data.

The school has a clear policy and procedures for automatic backing up, accessing and restoring of data held on school systems, including off-site backups.

7.1.2 Portable Devices

When personal data is stored on any portable computer system, USB stick or any other removable media, the portable computer system, USB stick or any other removable media will be supplied, fully encrypted, by the school.

The following will apply in EVERY case:

- the data must be encrypted and password protected / verified via MSU Team
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected) and verified via the MSU Team
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

7.1.3 Passwords

- All users will use strong passwords, (including 14 characters, a Capital letter, number and symbol) which must be changed regularly.
- User passwords will never be shared.
- Users will NOT record complete passwords.

7.1.4 Images

- Images of pupils will never be processed off site and, where necessary, permission for this will be obtained in the privacy notice or other photographic permission notice.
- Images will be protected and stored in a secure area.

7.1.5 Cloud Based Storage

- The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, Google Apps and Onedrive) and is aware that data held in remote and cloud storage is still required to be protected in line with Data Protection requirements. This detail is contained within the school's ICT Policy.

- The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

See advice from the DfE below:
https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection- act

7.2 Third Party data transfers

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses are included in all contracts where data is likely to be passed to a third party as well as data processing agreements.

7.3 Retention of Data

Please see School Retention Policy.

7.4 Systems to protect data

7.4.1 Paper Based Systems

All paper based personal data will be protected by appropriate controls, for example: -

- Paper based safeguarding chronologies will be in a locked cupboard when not in use.
- Class Lists used for the purpose of marking may be stored in a teacher's bag.
- Paper based personal information sent to parents will be checked by GDPR trained administrators, before the envelope is sealed.

7.4.2 School Websites

Uploads to the school website will be checked prior to publication, for instance: -
- to check that appropriate photographic consent has been obtained
- to check that the correct documents have been uploaded.

7.4.3 E-mail

E-mail cannot be regarded as a secure means of transferring personal data.

- All e-mails containing sensitive information will be encrypted, as a minimum, by attaching the sensitive information as a word document and encrypting the document / compressing and encrypting (the recipient will then need to contact the sender in school for access to a one off password). Recipients may, alternatively, receive a second email containing password detail.

School will ensure that, where special category data is shared, it is transmitted securely by encrypting the document / compressing and encrypting (the recipient will then need to contact the sender in school for access to a one off password) or is transferred in tamper proof envelopes securely delivered to the recipient via courier.

8. DATA SHARING

8.1. Sharing with the LA and DfE

The school is required by law to share information with the LA and DfE. Further details are available at: https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

8.2. Safeguarding

Schools MUST follow the statutory processes in Keeping Children safe in Education and Working together to Safeguard Children:
https://www.gov.uk/government/publications/working-together-to-safeguard-children--2

Durham Local Safeguarding Children Board provides information on information sharing at: http://www.durham-lscb.org.uk/wp-content/uploads/sites/29/2016/06/Guide-for-professionals-on-information-sharing.pdf

8.3. Transfer of Safeguarding and SEND records when a pupil moves school

The following is an extract from keeping Children safe in Education Sept 2018.

- Where children leave the school or college, the designated safeguarding lead should ensure their child protection file is transferred to the new school or college as soon as possible, ensuring secure transit, and confirmation of receipt should be obtained. For schools, this should be transferred separately from the main pupil file.

- Receiving schools and colleges should ensure key staff such as designated safeguarding leads and SENCOs or the named person with oversight for SEN in a college, are aware as required.

- In addition to the child protection file, the designated safeguarding lead should also consider if it would be appropriate to share any information with the new school or college in advance of a child leaving. For example, information that would allow the new school or college to continue supporting victims of abuse and have that support in place for when the child arrives.

9 DATA BREACH - Procedures

On occasion, personal data may be lost, stolen or compromised. Data breaches include both electronic media and paper records. It can also refer to inappropriate access to information.

- In the event of a data breach, the Data Protection Officer will inform the Headteacher and Chair of Governors.
- When a personal data breach has occurred, the school must establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then the school must notify the ICO; if it's unlikely then we don't have to report it. However, if the school decide not to report the breach, we need to be able to justify this decision, and it will be documented.
- The school will report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If the school takes longer than this, we must give reasons for the delay.

- If a breach is likely to result in a high risk to the rights and freedoms of individuals, GDPR states we must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible. A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO.
- In relation to data breaches, the school will follow the procedures set out below. This breach procedure sets out the course of action to be followed by all staff at Durham Johnston School if a data protection breach takes place.

9.1 Data Breach Statement

Durham Johnston School holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by Durham Johnston School and all school staff, Governors, volunteers and contractors, referred to herein after as 'staff'.

9.2 What is a potential data breach?

A potential data breach occurs, in general, when the GDPR 2018, is not complied with in the processing of personal information. Failure to comply with any of the 6 data protection principles can be considered a breach.

The 6 data protection principles are as follows:

1. 1a (Section 35 (1) Personal data shall be processed fairly, lawfully and in a transparent manner.

2. 1b Section 36 (1) Personal data shall be obtained only for one or more specified, explicit and legitimate and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. 1c Section 37 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. 1d Section 38 (1) Personal data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that Personal Data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

5. 1e Section 39 (1) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. 1f Section 40 Personal data processed for any of the law enforcement purposes must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organisational measures (and, in this principle, 'appropriate security' includes protection against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage.

9.3 Legal Context

Article 33 of the General Data Protection Regulations

Notification of a personal data breach to the supervisory authority:

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, **not later than 72 hours** after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:
   a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   c) describe the likely consequences of the personal data breach;
   d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

9.4 Types of Breach

A number of factors could cause data protection breaches. Examples are shown below:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error; Cyber-attack; Hacking.

9.5 Managing a Data Breach

In the event that the School identifies or is notified of a personal data breach, the following steps will be followed:

1. The person who discovers / receives a report of a breach **MUST** inform the DPO or nominated representative who will immediately inform the Chair of Governors and Headteacher.

2. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

3. The DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps will be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT Lead or Managed Service Unit.

4. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.

5. The DPO (or nominated representative) will also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the School's legal support will be obtained.

6. The DPO (or nominated representative) will quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

    a) Attempting to recover lost equipment.

    b) Contacting the relevant County Council Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration will be given to a global email to all school staff. If staff receive an inappropriate enquiry, they will attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the DPO (or nominated representative).

    c) Contacting the County Council's Communications Division / Crisis Service, so that they can be prepared to handle any press enquiries.

    d) The use of back-ups to restore lost/damaged/stolen data.

    e) If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

    f) If the data breach includes any entry codes or IT system passwords, then these will be changed immediately and the relevant agencies and members of staff informed.

9.6 Investigation

In most cases, the next stage would be for the DPO (or nominated representative) to fully investigate the breach. The DPO (or nominated representative) will ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation will consider:

- The type of data;
- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc.) and whether there are wider consequences **to the breach.**

A clear record will be made of the nature of the breach and the actions taken to mitigate it. The investigation will be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements will be carried out thereafter.

9.7 Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The DPO (or nominated representative) should, after seeking expert or legal advice, if necessary, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) will be notified within 72 hours of the breach. Every incident will be considered on a case-by-case basis.

When notifying individuals, specific and clear advice will be given on what they can do to protect themselves and what the School is able to do to help them. They will also be given the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure). The notification will include a description of how and when the breach occurred and what data was involved. It will include details of what has already been done to mitigate the risks posed by the breach.

9.8 Review and Evaluation

Once the initial aftermath of the breach is over, the DPO (or nominated representative) will fully review both the causes of the breach and the effectiveness of the response to it. Details will be reported to the next available Leadership Group meeting and Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan will be drawn up to put this right. If the breach warrants a disciplinary investigation, the manager leading the investigation will liaise with Human Resources or Internal Audit for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

9.9 Implementation

The DPO will ensure that staff are aware of the School's Data Protection policy and its requirements including this breach procedure. This will be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the School's Data Protection Policy and associated procedures, they should discuss this with their line manager, GDPR Team or Headteacher.

9.9.1 Data Breach Investigation Template

Please see Appendix 3.

10. SCHOOL CCTV CODE OF PRACTICE

10.1 Introduction

Durham Johnston School uses closed circuit television (CCTV) and the images produced to prevent or detect crime and to monitor the school buildings and grounds in order to provide a safe and secure environment for its pupils, staff and visitors, and to prevent loss or damage to school property.

The system comprises a number of fixed and dome cameras and does not have sound recording capability.

The CCTV system is owned and operated by the school, the deployment of which is determined by the school's Leadership Group.

The CCTV is monitored centrally from the Caretaker's office.

Access to the images is controlled by the Leadership Group and is password protected.

The school's CCTV Scheme is registered with the Information Commissioner under the terms of the Data Protection Act 1998. The use of CCTV and the associated images are covered by the Data Protection Act 2018. This code of practice outlines the school's use of CCTV and how it complies with the Act.

All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. Through this code of practice, all operators are made aware of their responsibilities.

The school's representative of the 'Data Controller' (Head Teacher) will ensure that all employees are aware of the restrictions in relation to access to, and disclosure of, recorded images by publication of this policy.

10.2 Statement of Intent

The school complies with the Information Commissioner's Office (ICO) CCTV Code of Practice to ensure that CCTV is used responsibly and safeguards both trust and confidence in its continued use.

CCTV warning signs are clearly and prominently placed at the main external entrance to the school, including further signage in other areas in close proximity to camera positions.

Signs contain details of the purpose for using where appropriate.

In areas where CCTV is used, the school will ensure that there are prominent signs placed within the controlled area.

The original planning, design and installation of CCTV equipment endeavoured to ensure that the scheme will deliver maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

10.3 Siting the Cameras

Cameras are sited so that they only capture images relevant to the purposes for which they are installed. Care will be taken to ensure that reasonable privacy expectations are not violated. The School will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act 2018/GDPR.

The school will make every effort to position cameras so that their coverage is restricted to the school premises, which includes outdoor/indoor areas.

CCTV will not be used in classrooms but in limited areas within the school building (i.e. meeting rooms, pastoral staff offices, Student Support Centre). These areas have been identified by staff and pupils as not being easily monitored at all times.

Members of staff will have access to details of where CCTV cameras are situated.

10.4 Covert Monitoring

No cameras are used for the purpose of routine covert monitoring. It is not the school's policy to conduct 'Covert Monitoring' unless there are 'exceptional reasons' for doing so.

The school may, in exceptional circumstances, determine a sound reason to set up covert monitoring. For example:

i. Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;

ii. Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

In these circumstances authorisation will be obtained from a member of the senior leadership group and the school's 'Data Controller' advised before any commencement of such covert monitoring.

Covert monitoring will cease following completion of an investigation.

Cameras sited for the purpose of covert monitoring will not be used in areas, which are reasonably expected to be private, for example toilet cubicles, changing areas etc.

10.5 Storage and Retention of CCTV images

Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

All retained data will be stored securely at all times and permanently deleted as appropriate / required.

10.6 Access to CCTV images

Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available.

Staff authorised to view images include the school caretaker who manages the CCTV system, Technical Officers (DCC Managed Service Unit) and Leadership Group members.

10.7 Subject Access Requests (SAR)

Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act/GDPR.

Please see Section 11 below for further detail.

10.8 Access to and Disclosure of Images to Third Parties / Complaints

There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators).

The data may be used within the school's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

Complaints and enquiries about the operation of CCTV within the school should be directed to the DPO / GDPR Team in the first instance.

10.9 CCTV - Further Information

Further information on CCTV and its use is available from the following:

- CCTV Code of Practice Revised Edition 2017 (published by the Information
- Commissioners Office) Version 1.2
- www.ico.org.uk
- Regulation of Investigatory Powers Act (RIPA) 2018
- Data Protection Act 2018
- GDPR (25 May 2018)
- Protection of Freedoms Act 2012

11. SCHOOL PHOTOGRAPHY CODE OF PRACTICE

This code of practice covers the recording, use, storage and deletion of still and video images at the school. Any examples used are not exhaustive and the school is able to make decisions on a case-by-case basis.

11.1 Legal Context

Legally this area is covered by the following:

- Data Protection Act 2018: The image of a pupil is personal data covered by the act unless taken by parents/carers for purely personal use. This means that a school must comply with the Data Protection Act 2018. In practice, a school will need to seek permission to take, use and store and display images when this forms part of the public task of educating children, disposing of them after the child has left. Schools will need to seek consent for other uses of images such as websites social media or newspapers.
- Education Act 2002: Obligations to safeguard the welfare of pupils. This may have an impact on pupils whose location cannot be revealed for safeguarding reasons.
- Article 8 European Convention on Human Rights: Privacy issues/breach of the pupil's right to respect for private life. For example, a parent/carer may object to their pupil's image being taken or shared.
- Article 10 European Convention on Human Rights: The parent/carer's right to freedom of expression.

11.2 Safeguarding

Safeguarding of young people will always take precedence when considering when photographs and videos are appropriate. In particular, we need to consider if we have pupils who:

- are looked after, particularly if the parents of the pupil are not allowed access
- are adopted
- are in protected accommodation
- have a parent or family member who is not permitted access.

11.3 Permission to Take and Use Images

- Consent is not required when the use of images if purely for educational purposes, for instance for assessment of learning. This is covered as part of the "Public Task" of the school.

- Consent will be required when images are used beyond the school, for instance on the school website. Consent shall be obtained from parents/carers at the start of every school year. It is good practice to ensure that the record of consent is approved as accurate and up to date by the parent/carer on a regular basis.

- A record of all consent details will be kept securely on file. Should parents/carers withdraw permission at any time, then all relevant images will be removed and disposed of and the record will be updated accordingly.

- Images will not be taken of any pupil or young person against their wishes. A pupil or young person's right not to be photographed will be respected.

- School visitors may only take photographs with the specific permission of a member of the school's Leadership Group when consent has been correctly obtained.

11.4 Taking, Storing and Retention of Images and Videos

As images and videos are personal data, they will be processed in accordance with the school's data protection policy.

Only official school owned equipment (e.g. school owned digital or video cameras) will be used by staff to capture images of pupils for official purposes. **Use of personal cameras or phones or other devices, for the purpose of photography or video making, by staff is prohibited at all times.**

Staff will receive information regarding the safe and appropriate use of images as part of their safeguarding training and responsibilities.

Images will be stored securely, for example, by using password protection, restricting the number of people who have access to the files, and ensuring adequate firewall and anti-virus software are in place. If the device is portable this will be encrypted (e.g. iPad with passcode).

Images will be securely deleted from non-encrypted devices on a regular basis (e.g. transferred from a digital camera to the network on a weekly basis).

Images will not be kept for longer than is considered necessary, and in any event, not exceeding a maximum of three years after the pupil has left the school. A designated member of staff (GDPR Advisor) will ensure that systems exist so that all photographs are permanently wiped from memory cards, computer hardware and portable drives or other relevant devices once the images will no longer be of use.

The school's Leadership Group reserve the right to view any images taken. Members of staff (including volunteers) will ensure that all images are available for scrutiny and will be able to justify any images in their possession.

11.5 Processing Images Off-Site

No image will be removed off-site either in hard copy or electronic format.

The school will ensure that any use of a cloud based storage system complies with the requirements of the school's data protection policy. The school will comply with the Information Commissioner's Office Guidance on the use of cloud computing.

11.6 Use of Images/Videos by Pupils

The school will discuss and agree age appropriate acceptable use rules with pupils regarding the appropriate use of cameras, such as, places pupils cannot take the camera (e.g. unsupervised areas, toilets etc.).

All staff will be made aware of the acceptable use rules regarding pupils' use of cameras and will ensure that pupils are appropriately supervised when taking images for official or curriculum use.

Members of staff will act as role models of positive behaviour to the pupils by encouraging them to ask permission before they take any photos.

Photos taken by pupils for official use will only be taken with parental/carer consent and will be processed in accordance with the Data Protection Act 2018.

Parents/carers will be made aware that pupils will be taking photos/videos of other pupils and will be informed how these images will be processed.

11.7 School Trips

Volunteers helping on school trips must be made aware of any rules restricting the use of personal devices to take photographs. This is the responsibility of the trip leader.

The school will decide if pupils are allowed to use their own cameras, phones, tablets and other connected devices, during a school trip on an individual event basis.

Pupils may not take personally owned cameras including disposable AND/OR digital cameras on school trips. Staff will monitor this requirement and any personally owned cameras including disposable AND/OR digital cameras may be confiscated.

Personally owned tablets, phones and other connected devices are not permitted to be used on school trips due to difficulties supervising the suitability of images shared over the internet.

11.8 Appropriate Events and Locations

There are some risks involved when taking photographs of some sporting occasions when pupils are not fully dressed. These apply to both the pupil, whose image may be misused, as well as the adult who could be accused of taking inappropriate images. The general advice is that pupils should not be photographed unless appropriately dressed.

It is never permissible to record images when pupils are changing or wearing swimming costumes.

11.9 Use of Webcams/Skype etc.

Parental/carer consent will be obtained before webcams or video conferencing will be used for curriculum or educational purposes.

Recordings will only be made with the consent of all parties taking part.

11.10 School Website/School Managed Social media

Permission will be obtained from parents/carers before a pupil's image is uploaded to the school website or social media platform.

Pupils' full names will not be used on the website or Social Media in association with photographs.

The school will not include any personal addresses, emails, telephone numbers, on videos, on the website, in a prospectus or in other printed publications.

Pupils' work will only be published with their consent or their parent /carer's consent.

11.10.1 Parental/Carer Photography

Many parents/carers will want to record some of the special moments in their pupil's school life and the law does not prohibit this. However, it is possible that they will also capture images of pupils other than their own child, with a possible impact on their privacy.

This is a problematic area with contributory factors:

- Freedom – some parents/carers will want to take pictures of their pupil at an event, and some will not.
- Privacy - it is possible that any image captured may have other pupils in it.
- Safeguarding – there is potential for images to be misused. There can be particular concern regarding looked after pupils

THE SCHOOL DOES NOT ALLOW PARENTAL / CARER / VISITOR / STUDENT PHOTOGRAPHY OR VIDEO AT ANY SCHOOL EVENT OR ACTIVITY.

The school will ensure that parents / carers / visitors and students are aware of restrictions on photography and video and will publicise this prior to the event, where needed, and bring it to the attention of parents / carers / visitors / students at the start of the event.

Parents/carers have the right to ask for their child not to be photographed. On some occasions that may result in the pupil being unable to take a full part in an activity.

11.10.2 Social Media

Uploading pictures to social media may cause further complications. A parent/carer publically sharing images of other pupils with no controls on privacy may be in breach of data protection rules. However, sharing images of their own child is not a breach of data protection rules.

THE SCHOOL DOES NOT ALLOW ANY IMAGES OR VIDEOS TO BE SHARED ON SOCIAL MEDIA AS IT CONSIDERS IT TO BE A RISK TO INDIVIDUAL PUPILS, PARENTS, CARERS, VISITORS AND STAFF PRIVACY.

We will challenge any public publishing of our students' images that comes to our attention if we feel it does not meet our safeguarding obligations.

Please be aware, there might be pupils alongside your child who are vulnerable to having their image distributed.

11.10.3 Press Photography

Where a press photographer is to be invited to celebrate an event, every effort will be made to ensure that the newspaper's (or other relevant media's) requirements can be met. A written agreement will be sought between parents/carers and the press which will request that a pre-agreed and accepted amount of personal information (e.g. first names only) can be published along with images and videos.

The identity of any press representative will be verified and access will only be permitted where the event is planned, and where press are to be specifically invited to attend. No authorisation will be given to unscheduled visits by the press under any circumstances.

The photographer will be issued with visitor identification, which must be worn at all times.

Every effort will be made to ensure the press abide by any specific guidelines should they be requested. No responsibility or liability however can be claimed for situations beyond reasonable control, and where the school is to be considered to have acted in good faith.

11.10.4 School Photographs

Professional photographers who are engaged to record any events will be prepared to work according to the terms of the school's e-Safety policy.

Photographers will be issued with visitor identification, which must be worn at all times.

Photographers will sign an agreement, which ensures compliance with the Data Protection Act and confirms that images will only be used for a specific purpose, subject to parental/carer consent.

Photographers will not have unsupervised access to pupils and young people.

11.10.5 Photographs by Members of the Public

When pupils are taken out of the school grounds, for instance, on a visit it is possible that they could be photographed by members of the public. If the pupil's privacy is of paramount importance, the risk of this should be discussed with parents/carers and appropriate steps taken (see Looked After Pupils section below).

11.10.6 Looked After Pupils

Photographs of looked after pupils should usually only be taken with the agreement of the person who holds parental responsibility. However, in some circumstances, consent could be obtained from the pupil's social worker, foster carer or a relative. Please see the school/relevant teacher who is part of the pupil's care team if you are unsure about who can give consent.

The school/relevant teacher will be part of a looked after pupil's care team and attend meetings and looked after reviews; they should know any potential risks regarding any adults or if the placement is protected.

Looked after pupils should expect to have as normal an experience as they can and they should never be singled out because they are in care.

If a pupil's identity or privacy need to be protected, this should be discussed with the parent/carer and appropriate steps could be agreed. This could include:-

- Restricting parental photography at events
- Siting the pupil with the teacher to allow the teacher to take active steps to reduce the possibility of the pupil being photographed
- Sensitive withdrawal of the pupil from the event with an explanation to the pupil.

12. DATA PROTECTION IMPACT ASSESSMENTS

A Data Protection Impact Assessment (DPIA) is a key component of a 'Privacy by design' approach to any personal data processing activity (hereafter referred to as an 'initiative').
'Privacy by design' is an essential tool in minimising privacy risks and building trust. The Information Commissioner's Office (ICO) encourages organisations to ensure that privacy and data protection is a key consideration in the early stages of any initiative, and then throughout its lifecycle.

12.1 What is a Data Protection Impact Assessment (DPIA)?

A DPIA is a structured approach to identifying the privacy risks associated with the processing of personal data and for implementing appropriate controls to manage those risks. The process comprises the following six distinct steps and a parallel stream of consultation:

1. Identify the need for a DPIA
2. Describe the information flows
3. Identify and assess the privacy risks
4. Identify and approve controls
5. Assign responsibility for implementing controls
6. Re-assess and accept the risks.

12.2 Why conduct a DPIA?

Key benefits of conducting a DPIA are:

- Fulfilling the School's legislative, statutory and contractual obligations, particularly those under data protection legislation in relation to data processing activities
- Contributing towards effective risk management and increased privacy and data protection awareness across the School
- Giving individuals confidence that the School is taking steps to safeguard their privacy, and a better understanding of the ways in which their personal data are being used
- Taking actions which are less likely to be privacy intrusive and have a negative impact on individuals
- Increasing the likelihood that the initiative is more successful because privacy risks are identified early, allowing controls to be designed in at less cost and with less impact on delivery.

12.3 Is a DPIA required?

A DPIA should be completed for any initiative that involves the processing of personal data or any other activity that could affect the privacy of individuals. Examples are:

- Building a new IT system for storing or accessing staff personal data
- Implementing surveillance technology in a building, such as an additional CCTV system
- Using a cloud service for the storage of data
- Developing policies or strategies that have privacy implications.

A DPIA should be completed for new initiatives or for changes to existing systems or processes. It may also be a recommended outcome from a formal investigation into an information security incident or weakness at the School.

The first step in conducting a DPIA is a screening process to decide whether the detailed work in the subsequent steps will be required.

A DPIA must be completed for all projects that may affect the privacy of individuals and/or involve the use of personal data.

12.4 When should a DPIA be undertaken?

A DPIA should be undertaken in the early stages of an initiative. The earlier a DPIA is completed, the easier it is likely to be to address any privacy risks identified.

12.5 Who should conduct a DPIA?

The School Data Protection Officer has overall accountability for ensuring that DPIAs are completed for high-risk personal data processing initiatives.

Responsibility for ensuring that a specific DPIA is completed lies with the individual responsible for the initiative, such as:

- The project sponsor
- The information asset owner
- The lead for a project.

12.6 Who should hold the completed DPIA?

The individual responsible for the initiative should retain a copy of the completed DPIA for audit purposes and to be able to demonstrate compliance with legislative requirements should a query be raised. The School's GDPR Team will also hold a copy of the DPIA for monitoring and reporting purposes. Copies will be held in the Director of Resource's office in the Central GDPR Master file.

12.7 The School's DPIA template

The School's standard Data Protection Impact Assessment Template will be used (see Appendix 4).

12.8 Conducting a DPIA

Step One - Identify the need for a DPIA
Complete the DPIA screening questions in the DPIA template. If the answer to any of the screening questions is 'Yes', a DPIA is required. Below are the screening questions, with some additional context and examples to help determine answers.

Question		Context	Example
1	Does the initiative involve evaluating or scoring individuals (including profiling and predicting)?	This is particularly important when personal data processing relates to an individual's performance, economic situation, health, personal preferences or interests, relaibility or behaviour, location or movements.	Building behavioural or marketing profiles of individuals based on their web activity.
2	Does the initiative involve automated decision-making that may have a significant effect on an individual?	This is personal data processing that aims to make automated decisions about individuals that produce legal effects or similarly significant effects upon the individual.	Asking an individual to submit personal data that is then analysed by a computer system, with the result that the individual's request to use a service is either accepted or refused.
3	Does the initiative involve systematic monitoring?	This is personal data processing used to observe, monitor or control individuals.	Installing a CCTV system on School premises.
4	Does the initiative involve the processing of 'sensitive personal data'?	Sensitive personal data is a particular set of personal data, as defined by data protection legislation.	Processing the health data of staff in an absence related research project.

5	Does the initiative involve processing personal data on a large scale?	There is no specific definition of 'large scale' but the following should be considered: The number of individuals affected The volume of personal data The range of personal data The duration or permanence of the processing activity The geographical extent of the processing activity.	Implementing a new student record system.
6	Does the initiative involve datasets that have been matched or combined?	This relates to combining personal data originating from two or more personal data processing operations performed for different purposes or by different data controllers in a way that would exceed the reasonable expectations of the individual.	Matching alumni personal data against personal data held by a third party for profiling purposes.
7	Does the initiative involve the personal data of vulnerable people?	This relates to the processing of personal data where there is an imbalance of power between the individual and the School, or the processing involves a vulnerable section of society.	Processing children's personal data as part of a 'widening participation' activity in the School.
8	Does the initiative involve the use or application of innovative technological or organisational solutions?	New technology can often involve novel ways of collecting and using personal data that individuals may not reasonably expect.	Using fingerprint recognition technology to control access to the School building.
9	Does the initiative involve the transfer of personal data outside of the European Union?	This relates to sending personal data to countries outside of the European Union.	Storing personal data in a cloud service hosted in the USA.
10	Does the initiative prevent individuals from exercising a right or using a service or contract?	This includes personal data processing that takes place in a public area that passers-by cannot avoid, or processing that aims to allow or refuse an indidvidual's access to a service.	Screening applicants before allowing them to use a web service

Step Two - Describe the information flows
Record the following in the DPIA template:

- How personal data will be obtained
- How personal data will be processed (including potential future uses)
- How personal data will be stored
- To whom personal data will be disclosed (individuals or organisations, if any).

N.B. Consultation should begin during this step

Step Three - Identify and assess the privacy risks
Record the identified risks in the DPIA template. This forms the core of the DPIA process. The aim is to compile a comprehensive list of all of the privacy risks associated with the initiative, whether or not the risks require action.

For each privacy risk identified, the following should be recorded:

- A unique identifier
- A description of the risk
- An assessment of the impact of the risk (severe, major, moderate, minor, insignificant)
- An assessment of the likelihood of the risk (very likely, likely, neither likely nor unlikely, unlikely, very unlikely).

Step Four - Identify and approve the controls
Identify controls to mitigate the risks and record them in the DPIA template. The aim is to identify sufficient controls to eliminate each of the risks identified in Step Three, or to reduce them to a level, which is acceptable to the School.
For some identified risks, no controls may be required because the likelihood is so low and/or the impact so small that the risks are acceptable to the School.

Controls may take many forms, such as:

- Additional terms and conditions in a contract
- A privacy notice
- Documented operational procedures
- Disabling certain product features
- User training
- Technical controls, such as encryption.

Once a control is identified, the expected result of its implementation should be recorded i.e. whether it is likely to:

- Eliminate the risk
- Reduce the risk to an acceptable level
- Require acceptance as there is no reasonable control to eliminate or reduce it.

An appropriate individual should then approve proposed controls. Normally this should be the information asset owner or their nominated delegate, but it could also be the chair of a relevant Governing Body committee.

Step Five - Assign responsibility for implementing controls
Allocate the controls to appropriate individuals and record an agreed deadline for implementation.
In the case of formal School projects, the implementation of many of the controls will fall within the scope of the project, so should be managed in the same way as any other project task.

However, the implementation of some controls will be beyond the scope of the project (such as a change to School policy) so related tasks should be assigned through the School's normal management processes and added to the list of project dependencies.

Where initiatives are being run informally, or as 'business as usual' activities, the School's normal management processes should be used to identify who will implement the controls and agree an appropriate deadline. In all cases, a named individual and deadline for completion should be assigned and recorded.

In the absence of formal project management documentation, the DPIA should be used to record when controls are implemented.

Step Six - Re-assess and accept the risks
After the controls have been implemented, re-assess the risks and record the outcome in the DPIA template. The risks then need to be accepted by an appropriate individual. Normally this should be the information asset owner or their nominated delegate, but it could also be the chair of a relevant Governing Body committee.

The individual who signs off the risks should have a clear understanding of the initiative, particularly the privacy risks and how the controls address them. If any risk has not been reduced to an acceptable level after implementation of the controls identified in Step Four, additional controls will need to be identified and Step Five and Step Six will need to be repeated.

12.9 Consultation

Consultation serves many purposes throughout the DPIA process, such as:

- Explaining the initiative to stakeholders
- Explaining to stakeholders how the DPIA process will be used within the initiative to manage privacy risks
- Establishing current working practices that the initiative aims to update or replace
- Establishing how the new system or process is likely to be used in practice and in the case of general purpose facilities, their likely purpose
- Establishing the privacy concerns of stakeholders
- Soliciting suggestions for controls
- Explaining identified controls to stakeholders

Key stakeholders are likely to include:

- Individuals who understand the initiative from a technical point of view and in terms of personal data processing
- Individuals who will be using the new system or process
- Individuals whose personal data will be processed by the new system or process
- Collaborative partners
- The suppliers of a system
- The School's GDPR Team and DCC Legal Services.

NOTE: In cases where the impact of a risk identified at Step Three is assessed to be either severe or major and likelihood is assessed to be either likely or very likely, the School's Data Protection Officer must be consulted. If any risk remains at this level after the implementation of controls, the School may be required to consult the Information Commissioner's Office

13. SUBJECT ACCESS REQUESTS

Subject Access Requests (SAR) deal with the rights of individuals to access their personal data. It also clarifies what we must do in this regard to comply with our duties as a data controller.

These rights and duties are set out in section 45 of the Data Protection Act 2018 (DPA) and are often referred to as 'the right of subject access'.

13.1 Subject Access Request (SAR) Format & Validity

You have the right to request a copy of the personal data the school holds about you. You might not want all of the personal data that the school holds about you and we may be able to respond more quickly if you explain this and identify the specific data you want.

When making a subject access request (SAR), which can be made verbally or in writing, please include the following information:

- **Your name and contact details**

- **Any details or relevant dates that will help the school to identify what you want.**

We are required to respond within 1 month of your request (and up to 2 months beyond this for very exceptional circumstances). If we cannot respond within 1 month we will write to you to tell you this and explain the reason(s) for it, however our aim is to respond to you within 15 days. We may be able to respond more quickly to your request if you contact us via the following email address: gdprteam@durhamjohnston.org.uk.

The school is entitled to satisfy itself as to the identity of the person making the request. The requester must provide evidence of their identity, we will ask you to send or bring in proof of ID including proof of address and a recognised form of photo ID (i.e. passport, driving licence).

The request does not have to include the words 'subject access' or make any reference to the DPA. Indeed, a request may be a valid SAR even if it refers to other legislation, such as the Freedom of Information Act (FOIA).

An emailed or verbal SAR request is as valid as one sent in hard copy. SARs might also be received via social media and possibly via third-party websites.

If a request does not mention the DPA specifically or even say that it is a subject access request, it is nevertheless valid and will be treated as such if it is clear that the individual is asking for their own personal data.

Requesters do not have to tell the school their reason for making the request or what they intend to do with the information requested, although it may help the school to find the relevant information if requesters explain the purpose of the request. A request is valid even if the individual has not sent it directly to the person who normally deals with such requests. All school colleagues will be trained to recognise a SAR and deal with it in accordance with the school's SAR process.

Individuals may make a SAR using any Facebook page or Twitter account the school has, other social-media sites to which it subscribes, or possibly via third-party websites. This might not be the most effective way of delivering the request in a form we will be able to process quickly and easily, but there is nothing to prevent it in principle.

The school may decline to use social media to supply information in response to a SAR if technological constraints make it impractical, or if information security considerations make it inappropriate to do so. In these circumstances we will ask for an alternative delivery address for the response.

The DPA does not prevent an individual making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual wants someone else to act for them.

In these cases, the school will need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

If the school thinks an individual may not understand what information would be disclosed to a third party who has made a SAR on their behalf, we may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

In some cases an individual does not have the mental capacity to manage their own affairs. There are no specific statutory provisions enabling a third party to exercise subject access rights on such a person's behalf. It is reasonable for the school to assume that an attorney with authority to manage the individual's property and affairs, or a person appointed by the Court of Protection to make decisions about such matters, will have the appropriate authority.

Even if a child is too young to understand the implications of subject access rights, data about them is still their personal data and does not belong to 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, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

13.2 SAR Fee

We cannot charge a fee to comply with a subject access request.

However, where the request is manifestly unfounded or excessive we may charge a "reasonable fee" for the administrative costs of complying with the request.

13.2.1 Information Held About Pupils in Schools

A pupil, or someone acting on their behalf, may make a SAR in respect of personal data held about the pupil by a school. If the school is in England, Wales or Northern Ireland, the SAR should be dealt with by the school.

There are two distinct rights to information held about pupils by schools. They are:

- the pupil's right of subject access under the DPA; and
- the parent's right of access to their child's 'educational record' (in England, Wales and Northern Ireland this right of access is only relevant to maintained schools – not independent schools, English academies or free schools).

It is important to understand what is meant by a pupil's 'educational record'. This is because there is an overlap between the two rights mentioned above.

The law on educational records does not lie within the regulatory responsibilities of the Information Commissioner.

The statutory definition of 'educational record' differs between England and Wales, Scotland and Northern Ireland. Broadly speaking, however, the expression has a wide meaning and includes most information about current and past pupils that is processed by or on behalf of a school. However, information kept by a teacher solely for their own use does not form part of the educational record. It is likely that most of the personal information a school holds about a particular pupil will form part of the pupil's educational record. However, it is possible that some of the information could fall outside the educational record; e.g. information about the pupil provided by the parent of another child is not part of the educational record.

Unlike the distinct right of access to the educational record, the right to make a SAR is the pupil's right. Parents are only entitled to access information about their child by making a SAR if the child is unable to act on their own behalf or has given their consent.

If it is not clear whether a requester has parental responsibility for the child or is acting on their behalf, the school will clarify this before responding to the SAR.

In deciding what information to supply in response to a SAR, the school needs to have regard to the general principles about exemptions from subject access.

Examples of information which (depending on the circumstances) it might be appropriate to withhold include:

- information that might cause serious harm to the physical or mental health of the pupil or another individual;
- information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests;
- information contained in adoption and parental order records; and certain information given to a court in proceedings concerning the child.

13.2.3 Information about Examinations

Special rules apply to SARs relating to information about the outcome of academic, professional or other examinations. These rules, which apply to requests for examination scripts, marks or markers' comments, are designed to prevent the right of subject access being used as a means of circumventing an examination body's processes for announcing results.

Information comprising the answers given by a candidate during an examination is exempt from the right of subject access. So a SAR cannot be used to obtain a copy of an individual's examination script.

Although this exemption does not extend to an examiner's comments on a candidate's performance in an examination (whether those comments are marked on the examination script or recorded on a separate marking sheet), or to details of the marks awarded, there is a special rule governing the time limit for responding to a SAR for such information in cases where the SAR is made before the results are announced. In such cases, a response must be provided within the earlier of:

- five months of the date of the request; and
- 40 days of the date on which the results are announced.

Where a SAR is made for an individual's examination marks, a response may only be refused (or delayed) for reasons permitted by the DPA.

Clearly, though, providing information about examination results is not the same as conferring a qualification.

13.3 What Information is an Individual Entitled to

Subject access is most often used by individuals who want to see a copy of the information an organisation holds about them. However, subject access goes further than this and an individual is entitled to be:

- told whether any personal data is being processed;

- given a description of the personal data, the reasons it is being processed and whether it will be given to any other organisations or people;
- given a copy of the personal data; and
- given details of the source of the data (where this is available).

An individual can also request information about the reasoning behind any automated decisions taken about him or her, such as a computer-generated decision to grant or deny credit, or an assessment of performance at work (except where this information is a trade secret).

Subject access provides a right for the requester to see their own personal data, rather than a right to see copies of documents that contain their personal data. Often, the easiest way to provide the relevant information is to supply copies of original documents, but we are not obliged to do this.

13.4 Time Limit

The school must act on the subject access request without undue delay and at the latest within one month of receipt. The school will also send an acknowledgement of the request within 15 days.

For the full response, the school calculates the time limit from the day after we receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

For practical purposes, if a consistent number of days is required (e.g. for operational or system purposes), we will adopt a 28-day period to ensure compliance is always within a calendar month.

The school can extend the time by up to 2 months to respond if the request is complex or we have received a number of requests from the individual. We must let the individual know within one month of receiving their request and explain why the extension is necessary.

However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:

- it is manifestly unfounded or excessive;
- an exemption applies; or
- we are requesting proof of identity before considering the request.

If the school have doubts about the identity of the person making the request we can ask for more information. However, it is important that we only request information that is necessary to confirm who they are. The key to this is proportionality. Should the school require additional proof of identity, we will let the individual know as soon as possible that we need more information from them to confirm their identity. The period for responding to the request then begins when we receive the additional information.

13.5 Monitoring Compliance

Compliance with SAR requirements will be the responsibility of the representative of the data controller (i.e. Headteacher).

Compliance with SAR requirements will be formally monitored and discussed at relevant governance meetings.

Management information will be kept showing the number of SARs received.

Details of any requests that have not been actioned within the statutory time limit will be escalated to the Headteacher and a suitable governance forum, so that any breach is tackled at a high level.

14. Policy Review:

This policy will be reviewed, and updated if necessary every year or when legislation changes.

Date:	**Review:**
Signed: ***Chair of Governors***	
Adopted by the Governing Body on:	
The Data Protection Officer is provided by Judicium Education	

Appendix 1 - Links to resources and guidance

ICO Guidance on GDPR
Specific information for schools is available here. This includes links to guides from the DfE

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

http://ico.org.uk/for_organisations/sector_guides/education

Specific Information about CCTV
http://ico.org.uk/for_organisations/data_protection/topic_guides/cctv

Information and Records Management Society – Schools records management toolkit
A downloadable schedule for all records management in schools
http://irms.org.uk/page/SchoolsToolkit

Disclosure and Barring Service (DBS)
Details of storage and access to DBS certificate information.
https://www.gov.uk/government/publications/handling-ofdbs-certificate-information/handling-of-dbs-certificate-information

DFE
GDPR Toolkit
https://www.gov.uk/government/publications/data-protection-toolkit-for-schools

Privacy Notices
https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

Use of Biometric Data
https://www.gov.uk/government/publications/protection-of-biometric-information-of-pupils-inschools

Safeguarding
https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
and
https://www.gov.uk/government/publications/working-together-to-safeguard-children--2

Appendix 2 - Glossary

GDPR - The General Data Protection Regulation. These are new European-wide rules that are the basis of data protection legislation. They are enforced in the UK by the ICO.

Personal data (as defined by the Data Protection Act 2018)
Data that relates to a living individual who can be identified from that data, or from that data and other information that comes into the possession of the Data Controller. For example:

- Name
- Address and postcode
- Date of birth

Sensitive personal data (as defined by the Data Protection Act 2018 and GDPR) Personal data consisting of:

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Genetic or Biometric Data

Data Controller
A person or organisation that determines the purposes for which, and the manner in which, personal information is to be processed. The school should be registered as a Data Controller.

Data Processor
A person who processes personal information on a data controller's behalf. Anyone responsible for the disposal of confidential waste is also included under this definition.

Data Subject
The living individual who is the subject of the data/personal information.

Potential Data Breach
The potential loss, theft, corruption, inappropriate access or sharing of personal, or sensitive personal data.

Ransomware
Illegal software that encrypts users' data, then holds the school to ransom demanding payment of hundreds of pounds to provide the password.

Data Protection Act 1998: DPA 2018 supports GDPR rather than enacting it, the 2 laws should be read together
All personal data which is held must be processed and retained in accordance with the eight principles of the Act and with the rights of the individual. Personal data must not be kept longer than is necessary (this may be affected by the requirements of other Acts in relation to financial data or personal data disclosed to Government departments). Retention of personal data must take account of the Act, and personal data must be disposed of as confidential waste. Covers both personal data relating to employees and to members of the public.

ICO:
The Information Commissioner's Office. This is a government body that regulates the Data Protection Act and GDPR
The ICO website is here http://ico.org.uk/

Data Protection Act 1998: Compliance Advice. Subject access – Right of access to education records in England:
General information note from the Information Commissioner on access to education records. Includes timescale (15 days) and photocopy costs.

Data Protection Act 1998: Compliance Advice. Disclosure of examination results by schools to the media:
General information note from the Information Commissioner on publication of examination results.

Education Act 1996:
Section 509 covers retention of home to school transport appeal papers. (By LA)

Education (Pupil Information) (England) Regulations 2005:
Retention of Pupil records

Health and Safety at Work Act 1974 & Health and Safety at Work Act 1972: Retention requirements for a range of health and safety documentation including accident books, H&S manuals etc.

School Standards and Framework Act 1998:
Retention of school admission and exclusion appeal papers and other pupil records.

Durham Johnston

Data Breach Investigation Report Template

Column A	Column B
Quick reference guide	**Type your investigation report in this column**
Incident Date	
Incident Number	
Author(s) / Investigating Officer	
Report Date	
Incident description and consequences (Concise incident description, including number of data subjects.)	
Information Recovered	
Decision as to whether those individuals whose data has been breached are to be notified.	
Chronology of events (For complex cases, any time line included in the report should be a summary.)	
Contributory factors (A list of significant contributory facts.)	
Root Causes (These are the most fundamental underlying factors contributing to the incident that can be addressed. Root causes should be meaningful and there should be a clear link, by analysis, between root CAUSE and EFFECT.)	

Lessons learned (Key issues identified which may not have contributed to this incident but from which others can learn.)	
Type of breach	Please tick one of the following: Near miss ☐ Potential breach ☐ Further action: *please provide details* ☐ No further actions ☐ Formal breach ☐
Recommendations (Numbered and referenced) Recommendations should be directly linked to root causes and lessons learned. They should be clear but not detailed. (Detail belongs in the action plan.) It is generally agreed that key recommendations should be kept to a minimum wherever possible. All recommendations are to be Specific, Measurable, Achievable, Realistic and Timely. – SMART.	
Arrangements for shared learning (Describe how learning has been or will be shared with staff and other organisations.)	
Outcome (The conclusion of the investigation should state whether the author believes the breach should be logged formally or not.)	
SIGNATURES **Headteacher, DPO and Chair of Governors** **Date**	

Durham Johnston

Data Protection Impact Assessment Template

DPIA author:	
Initiative title:	
Date completed:	

Context

Provide a brief explanation of the initiative - What is the initiative for? When is it likely to happen? How will it provide a benefit to the School? How will it provide a benefit to others?

Step One - Identify the need for a DPIA

Screening question	**Yes/No**
Does your initiative involve evaluating or scoring individuals (including profiling and predicting)?	
Does your initiative involve automated decision-making that may have a significant effect on an individual?	
Does your initiative involve systematic monitoring?	
Does your initiative involve the processing of sensitive personal data?	
Does your initiative involve processing personal data on a large scale?	
Does your initiative involve datasets that have been matched or combined?	
Does your initiative involve the personal data of vulnerable people?	
Does your initiative involve the use or application of innovative technological or organisational solutions?	
Does your initiative involve the transfer of personal data outside of the European Union?	
Does your initiative prevent individuals from exercising a right or using a service or contract?	

Based on the above information, it has been decided that a full DPIA [is / is not] required.

Step Two – Describe the information flows

Step Three – Identify and assess the privacy risks

Risk ID	Privacy risk	Impact	Likelihood

Step Four - Identify and approve controls

Risk ID	Control(s) identified	Expected result	Approved by

Step Five – Assign responsibility for implementing controls

Risk ID	Control(s)	Responsible officer	Deadline for implementation	Completion date

Step Six – Reassess and accept the risks

Risk ID	Privacy risk	Impact after control	Likelihood after control	Risk accepted by

Consultation

The conduct of this Data Protection Impact Assessment has involved the following consultation:

Contact for raising additional privacy concerns

Name:			
Job title:			
Email address:		Telephone:	