Peak Edge Group of Schools (PEGS)
Data Protection Policy

General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Policy Objectives
The school as the Data Controller will comply with its obligations under the GDPR and DPA. The school is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy.

The Information Commissioner as the Regulator can impose fines of up to 20 million Euros (approximately £17 million) for serious breaches of the GDPR; therefore it is imperative that the school and all staff fully comply with the legislation.

Scope of the Policy
Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information[1]. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the GDPR, personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

The school collects a large amount of personal data every year, including: pupil records, staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the school. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of local authorities (LAs), government agencies and other bodies.

The Principles
The principles set out in the GDPR must be adhered to when processing personal data:

[1] GDPR Article 4 Definitions

1. Personal data must be processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**).
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**).
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (**data minimisation**).
4. Personal data shall be accurate and, where necessary, kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (**accuracy**).
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (**storage limitation**).
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (**integrity and confidentiality**).

Transfer Limitation

In addition, personal data shall not be transferred to a country outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data as determined by the European Commission or where the organisation receiving the data has provided adequate safeguards[2].

This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer data where the data subject has provided explicit consent or for other limited reasons. Staff should contact the Data Protection Officer (DPO) if they require further assistance with a proposed transfer of personal data outside of the EEA.

Lawful Basis for processing personal information

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:

- Processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the school

- Processing is necessary for the performance of a **contract** to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract

[2] These may be provided by a legally binding agreement between public authorities or bodies, standard data protection clauses provided by the ICO or certification under an approved mechanism.

- Processing is necessary for compliance with a **legal obligation** to which the data controller is subject

- Processing is necessary in order to protect the **vital interests** of the data subject or of another natural person

- Processing is necessary for the purposes of the **legitimate interests** pursued by the data controller or by a third party[3]

- The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent must be kept separate from those other matters

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first consented.

The decision as to which lawful basis applies must be documented to demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for it in the school's relevant privacy notice(s).

When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside the school's public tasks) a legitimate interest assessment must be carried out and recorded. Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted.

Sensitive Personal Information
Processing of sensitive personal information (known as 'special categories of personal data') is prohibited[4] unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:
- There is a lawful basis for doing so as identified on previous page
- One of the special conditions for processing sensitive personal information applies:

[3] The GDPR states that legitimate interests do not apply to processing carried out by public authorities in the performance of their tasks, Article 6. However, the ICO indicates that where there are other legitimate purposes outside the scope of the tasks as a public authority, legitimate interests may be considered where appropriate (particularly relevant for public authorities with commercial interests).
[4] GDPR, Article 9

(a) the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject
(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
(d) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
(e) the processing relates to personal data which are manifestly made public by the data subject
(f) the processing is necessary for the establishment, exercise or defence of legal claims
(g) the processing is necessary for reasons of substantial public interest
(h) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services
(i) the processing is necessary for reasons of public interest in the area of public health.

The school's privacy notice(s) sets out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Unless the school can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that the school can demonstrate compliance with the GDPR.

Automated Decision Making

Where the school carries out automated decision-making (including profiling) it must meet all the principles and have a lawful basis for the processing. Explicit consent will usually be required for automated decision-making (unless it is authorised by law or it is necessary for the performance of or entering into a contract).

Additional safeguards and restrictions apply in the case of solely automated decision-making, including profiling. The school must, as soon as reasonably possible, notify the data subject in writing that a decision has been taken based on solely automated processing and that the data subject may request the school to reconsider or take a new decision. If such a request is received staff must contact the DPO, as the school must reply within 21 days.

Data Protection Impact Assessments (DPIA)
All data controllers are required to implement 'Privacy by Design' when processing personal data. This means the school's processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles.

Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA must be carried out to assess:

- whether the processing is necessary and proportionate in relation to its purpose
- the risks to individuals
- what measures can be put in place to address those risks and protect personal information

Staff should adhere to the Data Protection Toolkit for Schools from the DfE with reference to the DPIA template.

When carrying out a DPIA, staff should seek the advice of the DPO for support and guidance and once complete, refer the finalised document to the DPO for sign off.

Documentation and records

Written records of processing activities must be kept and recorded including:

- the name(s) and details of individuals or roles that carry out the processing
- the purposes of the processing
- a description of the categories of individuals and categories of personal data
- categories of recipients of personal data
- details of transfers to third countries, including documentation of the transfer mechanism safeguards in place
- retention schedules
- a description of technical and organisational security measures

As part of the school's record of processing activities the DPO will document, or link to documentation on:

- information required for privacy notices
- records of consent
- controller-processor contracts
- the location of personal information
- DPIAs and
- records of data breaches.

Records of processing of sensitive information are kept on:

- the relevant purposes for which the processing takes place, including why it is necessary for that purpose
- the lawful basis for our processing, and
- whether the personal information is retained or erased in accordance with the Retention Schedule and, if not, the reasons for not following the policy.

The school should conduct regular reviews of the personal information it processes and uptate its documentation accordingly. This may include:

- carrying out information audits to find out what personal information is held
- talking to staff about their processing activities, or
- reviewing policies, procedures, contracts and agreements to address retention, security and data sharing.

Privacy Notices

The school will issue privacy notices as required, informing data subjects (or their parents, depending on age of the pupil, if about pupil information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the GDPR including the identity of the data controller and the DPO, how and why the school will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the GDPR as soon as possible after collecting or receiving the data. The school must also check that the data was collected by the third party in accordance with the GDPR and on a basis which is consistent with the proposed processing of the personal data.

The school will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The school will issue a minimum of two privacy notices, one for pupil information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes.

These privacy notices can be found at:
<Insert link to your school pupil privacy notice>
<Insert link to your school workforce privacy notice>

Please note privacy notice templates can be found at:
www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

Data minimisation
Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.

The school maintains a Retention Schedule to ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the Schedule. This includes requiring third parties to delete such data where applicable.

Staff must ensure that data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Individual Rights
Staff as well as any other 'data subjects' have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed *(see the relevant privacy notice)*

- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request ('SAR' – see SAR Procedures, Appendix 2). Guidance on the ICO's 'Access to pupils' information held by schools in England' can be found at:

  https://schoolsnet.derbyshire.gov.uk/performance-information/data-protection-and-foi/information-governance.aspx

- To have data corrected if it is inaccurate or incomplete

- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')

- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where the school no longer need the personal information, but you require the data to establish, exercise or defend a legal claim

- To restrict the processing of personal information temporarily where you do not think it is accurate (and the school are verifying whether it is accurate), or where

you have objected to the processing (and the school are considering whether the school's legitimate grounds override your interests)

- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format

- To withdraw consent to processing at any time (if applicable)

- To request a copy of an agreement under which personal data is transferred outside of the EEA

- To object to decisions based solely on automated processing, including profiling

- To be notified of a data breach which is likely to result in high risk to their rights and obligations

- To make a complaint to the ICO or a Court

Individual Responsibilities
During their employment, staff may have access to the personal information of other members of staff, suppliers, clients or the public. The school expects staff to help meet its data protection obligations to those individuals.

If you have access to personal information, you must:

- only access the personal information that you have authority to access and only for authorised purposes
- only allow other staff to access personal information if they have appropriate authorisation
- only allow individuals who are not school staff to access personal information if you have specific authority to do so
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection, encryption and secure file storage and destruction in accordance with the school's policies)
- not remove personal information, or devices containing personal information (or which can be used to access it), from the school's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device
- not store personal information on local drives or on personal devices that are used for work purposes.

Information Security
The school will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow their school's acceptable usage policy.

The school will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation, where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the **confidentiality, integrity and availability** of the personal data, defined as follows:

- **Confidentiality** means that only people who have a need to know and are authorised to use the personal data can access it.

- **Integrity** means that personal data is accurate and suitable for the purpose for which it is processed.

- **Availability** means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the school has implemented and maintains in accordance with the GDPR and DPA.

Where the school uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of the school
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of the school and under a written contract
- the organisation will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to the school as requested at the end of the contract

- the organisation will submit to audits and inspections, provide the school with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the school immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

Storage and retention of personal information
Personal data will be kept securely in accordance with the school's data protection obligations.

Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained. Staff should adhere to the school's Records Retention Schedule. The Derbyshire Records Retention Schedule can be found at:

https://schoolsnet.derbyshire.gov.uk/performance-information/data-protection-and-foi/information-governance.aspx

Personal information that is no longer required will be deleted in accordance with the School's Record Retention Schedule.

Data breaches
A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Blagging offences where information is obtained by deceiving the organisation which holds it

The school must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. The school must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform their DPO/Head teacher immediately that a data breach is discovered and make all reasonable efforts to recover the information, following the school's agreed breach reporting process (see Appendix 1: 'School Data Breach Procedure').

Training
The school will ensure that staff are adequately trained regarding their data protection responsibilities.

Consequences of a failure to comply
The school takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the school, and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the school's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact your line manager or the school's DPO.

Review of Policy
This policy will be updated as necessary to reflect best practice or amendments made to the GDPR or DPA.

The Supervisory Authority in the UK
Please follow this link to the ICO's website (https://ico.org.uk/) which provides detailed guidance on a range of topics including individuals' rights, data breaches, dealing with subject access requests, how to handle requests from third parties for personal data etc.

Glossary

Automated Decision-Making (ADM): when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.

Automated Processing: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, which signifies agreement to the processing of personal data relating to them.

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It is responsible for establishing practices and policies in line with the GDPR. The school is the Data Controller of all personal data relating to its pupils, parents and staff.

Data Subject: a living, identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major systems or business change programs involving the processing of personal data.

Data Protection Officer (DPO): the person required to be appointed in public authorities under the GDPR.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (not just action).

General Data Protection Regulation (GDPR): General Data Protection Regulation (*(EU) 2016/679*). Personal data is subject to the legal safeguards specified in the GDPR.

Personal data is any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the school collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, school workforce privacy policy) or they may be stand-alone privacy statements covering processing related to a specific purpose.

Processing means anything done with personal data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, restriction, erasure or destruction.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal data relating to criminal offences and convictions.

A P P E N D I C E S

Appendix 1: Data Breach Procedures

Appendix 2: SARs Procedures

Appendix 3: DPIA Procedures

Acknowledgement:
This template policy is based on a document originally created by Kent County Council

Appendix 1

School Data Breach Procedure

***Important:** This procedure has been produced based on current General Data Protection Regulations (GDPR) information. As further updates are released this procedure may be updated to reflect the changes. The GDPR will apply in the UK from 25 May 2018*

Version History			
Version	**Date**	**Detail**	**Author**
1.0	11/10/2017	Completed for distribution	Children's Services School Support

Data Protection - Data Breach Procedure for [Insert name of school]

The following is a sample data protection breach procedure for schools to be adapted as required. It has been written to be included as an Annex/Appendix to the School's Data Protection Policy.

Policy Statement

[Insert name of 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 **[Insert name of school]** and all school staff, Governors, volunteers and contractors, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at **[Insert name of school]** if a data protection breach takes place.

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.

Types of Breach

Data protection breaches could be caused by a number of factors. A number of 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.

Managing a Data Breach

In the event that the school identifies or is notified of a personal data breach, the following steps should followed:

1. The person who discovers/receives a report of a breach must inform the Head Teacher or, in their absence, either the Deputy Head Teacher and/or the School's Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The Head Teacher/DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must 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 technician.

3. The Head Teacher/DPO (or nominated representative) must inform the Chair of Governors as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.

4. The Head Teacher/DPO (or nominated representative) must 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 should be obtained.

5. The Head Teacher/DPO (or nominated representative) must 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 should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details and confirm that they will ring back the individual making the enquiry. Whatever the outcome of the call, it should be reported immediately to the Head Teacher/DPO (or nominated representative).

    c. Contacting the County Council's Communications Division if part of the crisis service, so that they can be prepared to handle any press

enquiries. The Council's Senior Communications Officer can be contacted by telephone on (01629) 538234.

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 must be changed immediately and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the Head Teacher/DPO (or nominated representative) to fully investigate the breach. The Head Teacher/DPO (or nominated representative) should 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 should 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 should be made of the nature of the breach and the actions taken to mitigate it (use *Data Breach Record* for this purpose). The investigation should 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 can be done once the matter has been resolved.

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 Head Teacher/DPO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case-by-case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the school is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the school's

Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the Head Teacher/DPO (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Management Team and Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should 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.

Implementation

The Head Teacher/DPO should ensure that staff are aware of the School's Data Protection Policy and its requirements including this breach procedure. This should 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, DPO or the Head Teacher.

Appendix 2

Peak Edge Group of Schools (PEGS)
Subject Access Request (SAR) Procedures

1 Statement

1.1 All **data subjects** have rights of access to their **personal data**. This document sets out the procedure to be followed in relation to any requests made for the disclosure of **personal data processed** by the School.

2 Definition of Data Protection terms

2.1 All defined terms in this procedure are indicated in bold text, and a list of definitions is included in Appendix 1 to this procedure.

3 Recognising a subject access request

3.1 As the school **processes personal data** concerning **data subjects**, those **data subjects** have the right to access that **personal data** under Data Protection law. A request to access this personal data is known as a subject access request or SAR.

3.2 A **data subject** is generally only entitled to access their own **personal data**, and not to information relating to other people.

3.3 Any request by a **data subject** for access to their **personal data** is a SAR. This includes requests received in writing, by email, and verbally.

3.4 If any member of our **Workforce** receives a request for information they should inform the Headteacher and the Data Protection Officer (DPO) as soon as possible.

3.5 In order that the School is properly able to understand the nature of any SAR and to verify the identity of the requester, any requester making a request verbally should be asked to put their request in writing and direct this to the DPO.

3.6 A SAR will be considered and responded to in accordance with the Data Protection Law.

3.7 Any SAR must be identified to the DPO at the earliest opportunity.

4 Verifying the identity and the rights of a requester

4.1 OUR SCHOOL is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are, and is entitled to have access to the data requested.

4.2 Where the School has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of two or more of the following:

- Current passport
- Current driving licence

- Recent utility bill with current address
- Birth/marriage certificate
- P45/P60
- Recent credit card or mortgage statement

4.3 If the School is not satisfied as to the identity of the requester then the request will not be complied with, so as to avoid the potential for an inadvertent disclosure of **personal data** resulting in a data breach.

4.4 If the requester has no right of access to the **personal data** requested (see section *Sharing information with third parties*), e.g. a parent without a legal parental right and responsibility, the request will not be complied with, so as to avoid the potential for an inadvertent disclosure of **personal data** resulting in a data breach. In such a case, the School will notify (where the **data subject** is under the age of 12 years) the parent *with* parental responsibility of the request that has been made.

5 Fee for responding to requests

5.1 The School will usually deal with a SAR free of charge.

5.2 Where a request is considered to be manifestly unfounded or excessive, a fee may be requested. Alternatively, the School may refuse to respond to the request. If a request is considered to be manifestly unfounded or unreasonable the School will inform the requester of why this is considered to be the case.

5.3 A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged, taking into account the administrative costs of providing the information.

5.4 The School will always notify the requester of any fee to be charged before carrying out the request.

6 Time period for responding to SAR

6.1 The School has one month to respond to a SAR. This will run from:

a. the date of the request
b. the date when any additional identification (or other) information requested is received
c. receipt of payment of any required fee.

6.2 In circumstances where the School is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity, and in the case of a third party requester, the written authorisation of the **data subject** (if over 12 years of age - see below: *Sharing information with third parties*) has been received.

6.3 The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

6.4 Where a request is considered to be sufficiently complex as to require an extension of the period for response, the School will notify the requester within one calendar month of receiving the request, together with reasons as to why this is considered necessary.

7 Form of response

7.1 A requester can request a response in a particular form. In particular, where a request is made by electronic means, unless the requester has stated otherwise, the information should be provided in a commonly readable format.

8 Sharing information with third parties

8.1 **Data subjects** can ask that the School shares their **personal data** with another person, such as an appointed representative. In such cases, written authorisation, signed by the **data subject**, confirming which of their **personal data** they would like School to share with the other person, should be requested.

8.2 Equally, if a request is made by a person seeking the **personal data** of a **data subject**, and which purports to be made on behalf of that **data subject**, then a response must not be provided unless and until written authorisation has been provided by the **data subject** (or parent where the **data subject** is under the age of 12 years). The School should not approach the **data subject** directly but should inform the requester that it cannot respond without the written authorisation.

8.3 **Personal data** belongs to the **data subject**, and in the case of the **personal data** of a child, regardless of their age, the rights in relation to that **personal data** are theirs and not those of their parents. Parents, in most cases, do not have automatic rights to the **personal data** of their child. However, there are circumstances where a parent can request the **personal data** of their child without requiring the consent of the child. This will depend on the maturity of the child and whether the School is confident that the child can understand their rights. Generally, where a child is under 12 years of age, they are deemed not to be sufficiently mature as to understand their rights of access and a parent can request access to their **personal data** on their behalf.

8.5 In relation to a child who is 12 years of age or older, then provided that the School is confident that they understand their rights, and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the School will require the written authorisation of the child before responding to the requester or provide the **personal data** directly to the child in accordance with the process above.

8.7 In all cases the School should consider the particular circumstances of the case, and the above are guidelines only.

9 Withholding information

9.1 There are circumstances where information can be withheld pursuant to a SAR. These are specific exemptions and requests should be considered on a case-by-case basis.

9.2 Where the information sought contains the **personal data** of third party **data subjects** then the School will:

- Consider whether it is possible to redact information so that this does not identify those third parties, taking into account that it may be possible to identify third parties from remaining information
- If this is not possible, consider whether the consent of those third parties can be obtained
- If consent has been refused, or it is not considered appropriate to seek that consent, consider whether it would be reasonable in the circumstances to disclose the information relating to those third parties. If it is not, then the information may be

withheld.

9.3 The School will inform the requester of the reasons why any information has been withheld.

9.4 Where providing a copy of the information requested would involve disproportionate effort, the School will inform the requester, advising whether it would be possible for them to view the documents at the school, or it will seek further detail from the requester as to what they are looking for, e.g. key word searches that could be conducted to identify the information that is sought.

9.5 In certain circumstances information can be withheld from the requester, including a **data subject**, on the basis that it would cause serious harm to the **data subject** or another individual. If there are any concerns in this regard, then the DPO should be consulted.

10 Process for dealing with a subject access request

10.1 When a subject access request is received, the School will:

- Notify the DPO who will be responsible for overseeing the School's response.
- Acknowledge receipt of the request and provide an indication of the likely timescale for a response within 5 working days (see template at Appendix 2).
- Take all reasonable and proportionate steps to identify and disclose the data relating to the request.
- Never delete information relating to a subject access request, unless it would have been deleted in the ordinary course of events – it is an offence to amend or delete data following receipt of a SAR that would not have otherwise been so amended or deleted.
- Consider whether to seek consent from any third parties which might be identifiable from the data being disclosed.
- Seek legal advice, where necessary, to determine whether the School is required to comply with the request or supply the information sought.
- Provide a written response, including an explanation of the types of data provided and whether, and as far as possible for what reasons, any data has been withheld (see template at Appendix 3).
- Ensure that information disclosed is clear, and technical terms are classified and explained.
- Keep written records of all correspondence and all actions taken during the process of the SAR. It will be especially important to record all requests that have been received verbally.

Name of DPO: Claire McKenzie
Contact details: claire.fisher@me.com
07712634718

Appendix A – Definitions

Term	Definition
Data subjects	Data subjects, for the purpose of this procedure, include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
Personal data	Personal data means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data controllers	Data controllers are the people or organisations that determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Law. We are the data controller of all personal data processed in our school.
Processing	Processing is any activity that involves the use of data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.
Workforce	Includes any individual employed by school and those who volunteer in any capacity, including Governors.

Appendix B – SAR Acknowledgement Template

[On headed paper of data controller]

[ADDRESSEE]
[ADDRESS LINE 1]
[ADDRESS LINE 2]
[POSTCODE]

[DATE]

Dear [NAME OF DATA SUBJECT],

Acknowledgment of your data subject access request

Reference: [DATA SUBJECT ACCESS REQUEST REFERENCE NUMBER]

I write to acknowledge receipt of your request for personal information, which we are responding to under article 15 of the General Data Protection Regulation.

[I also acknowledge receipt of your [IDENTIFICATION] as confirmation of your identity.]

Your request was received on [DATE] and, unless there are grounds for extending the statutory deadline of one calendar month, we expect to be able to give you a response by [DATE].

The reference for your request is [REFERENCE NUMBER]. Please quote this on all correspondence concerning this request.

Yours sincerely

(Name of sender)
(School name)

Appendix C – SAR Response Template

(Delete/complete as appropriate)

[On headed paper of data controller]

[ADDRESSEE]
[ADDRESS LINE 1]
[ADDRESS LINE 2]
[POSTCODE]

[DATE]

Dear [DATA SUBJECT],

Response to your data subject access request dated [DATE OF REQUEST]

We write further to your request for details of personal data, which we hold in school, and our acknowledgment of [DATE WHEN REQUEST FIRST ACKNOWLEDGED BY LETTER].

We enclose all of the data to which you are entitled under the General Data Protection Regulation (GDPR), in the following format:
[DETAILS OF FORMAT IN WHICH DATA IS PROVIDED, WITH REASONS FOR CHOOSING THE FORMAT: PAPER COPIES **OR** ELECTRONIC COPIES ON A CD OR MEMORY STICK **OR** A NEW DOCUMENT WHICH HAS BEEN CREATED AND SETS OUT THE INFORMATION THAT CONSTITUTES PERSONAL DATA. WHERE THE SAR WAS MADE BY ELECTRONIC MEANS THE RESPONSE SHOULD BE PROVIDED IN A COMMONLY USED ELECTRONIC FORM.]

We have contacted the following departments and individuals in order to locate personal data held which is within the scope of a data subject access request under article 15 of the GDPR:
[LIST OF DEPARTMENTS AND METHODOLOGY FOR IDENTIFYING PERSONAL DATA]

We can confirm the following in relation to the areas covered under article 15 of the GDPR and data existing on the date when your request was made:

The purposes for which the personal data is processed:
[LIST OF PURPOSES]

The recipients or classes of recipients of personal data to whom the data has been or will be disclosed and the location of any recipients outside the EEA:
[LIST OF RECIPIENTS (BY NAME OR GENERIC CLASS) TO WHOM DATA DISCLOSED. NOTE WHICH COUNTRIES NON-EEA RECIPIENTS PROCESS DATA IN AND STATE THE ARTICLE 46 SAFEGUARDS IN PLACE.]

The categories of personal data concerned:

[LIST CATEGORIES]

The envisaged period for which the personal data will be stored, or the criteria used to determine that period:
[LIST RETENTION PERIODS]

Any information available to [DATA CONTROLLER] as to the source of the data:
[SOURCES OF DATA HELD]

The following automated decision-making is applied to the personal data:
[IDENTIFY AUTOMATED DECISION MAKING INCLUDING PROFILING AND PROVIDE MEANINGFUL INFORMATION ABOUT THE LOGIC INVOLVED AS WELL AS THE SIGNIFICANCE AND THE ENVISAGED CONSEQUENCES OF SUCH PROCESSING FOR THE DATA SUBJECT]

You have the following rights under the GDPR:

- the right to request rectification of inaccurate personal data; and
- in limited circumstances, the right to:
  - request erasure of the personal information;
  - request restriction of processing of the personal information; or
  - object to the processing of the personal information.

You will note that some of the information has been redacted. The reason for this is that the redacted information relates to [a] third part[y/ies] who have not consented to the sharing of their information with you.

Some information has not been provided as it is covered by the following exemptions:
[LIST EXEMPTIONS APPLIED]

If you are unhappy with this response, and believe School has not complied with legislation, please ask for a review by following our Complaints Procedure, details of which can be found on our website at [LINK] **OR** by contacting [INDIVIDUAL (COULD BE DPO OR OTHER APPROPRIATE POSITION)].

If you still remain dissatisfied following an internal review, you can appeal to the Information Commissioner, who oversees compliance with data protection law. You should write to: Customer Contact, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Yours sincerely,

(Name of sender)
(School name)

Appendix 3

School Privacy Impact Assessment Procedures

Important Note

This procedure document has been produced based on current General Data Protection Regulations (GDPR) information. As further updates are released this procedure may be updated to reflect the changes.

Version History			
Version	**Date**	**Detail**	**Author**
1.0	11/10/2017	Completed for distribution	Children's Services School Support

Privacy Impact Assessment Procedure for [Insert name of school]

The following is a sample privacy impact assessment procedure for schools to be adapted as required. It has been written to be included as an Annex/ Appendix to the School's Data Protection Policy.

1. Introduction

A privacy impact assessment (PIA) is a tool which can help **[Insert name of school]** identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

An effective PIA will allow **[Insert name of school]** to identify and fix problems at an early project stage, reducing the associated costs and damage to reputation which might otherwise occur.

This procedure explains the principles which form the basis for a PIA.

The main body of the procedure sets out the basic steps which the School should carry out during the assessment process.

Templates are at Annex A and B

2. What is a Privacy Impact Assessment (PIA)?

A PIA is a process which helps an organisation to identify and reduce the privacy risks of any project which involves personal data. To be effective a PIA should be used throughout the development and implementation of the School's project.

A PIA will enable the School to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.

3. When will a PIA be appropriate?

PIAs should be applied to all new projects, because this allows greater scope for influencing how the project will be implemented. A PIA can also be useful when planning changes to an existing system.

A PIA can also be used to review an existing system, but the School needs to ensure that there is a realistic opportunity for the process to implement necessary changes to the system. The main purpose of the PIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met.

Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice. This analysis can be tested by consulting with people who will be working on, or affected by, the project.

Conducting a PIA does not have to be complex or time consuming but there must be a level of rigour in proportion to the privacy risks arising. A PIA should be undertaken before a project is underway.

4. **What is meant by Privacy?**

Privacy, in its broadest sense, is about the right of an individual to be left alone.

It can take two main forms, and these can be subject to different types of intrusion:

- **Physical privacy** - the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.

- **Informational privacy** – the ability of a person to control, edit, manage and delete information about them and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages
.

5. Informational Privacy

This procedure is concerned primarily with minimising the risk of informational privacy - the risk of harm through use or misuse of personal information.

Some of the ways this risk can arise is through personal information being:

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long;
- disclosed to someone where the person who it is about does not want them to have it;
- used in ways that are unacceptable to or unexpected by the person it is about; or
- not kept securely.

Harm can present itself in different ways. Sometimes it will be tangible and quantifiable, for example financial loss or losing a job. At other times it will be less defined, for example damage to personal relationships and social standing arising from disclosure of confidential or sensitive information.

Sometimes harm might still be real even if it is not obvious, for example the fear of identity theft that comes from knowing that the security of information could be compromised. There is also harm which goes beyond the immediate impact on individuals. The harm arising from use of personal information may be imperceptible or inconsequential to individuals, but cumulative and substantial in its impact on society. It

might for example contribute to a loss of personal autonomy or dignity or exacerbate fears of excessive surveillance.

The outcome of a PIA should be a minimisation of privacy risk.

6. The Benefits of a PIA

The Information Commissioner's Office (ICO) promotes PIAs as a tool which will help organisations to comply with their DPA obligations, as well as bringing further benefits.

Whilst a PIA is not a legal requirement (except 'high risk processing i.e. safeguarding data), the ICO may often ask an organisation whether they have carried out a PIA. It is often the most effective way to demonstrate to the ICO how personal data processing complies with the DPA.

More generally, consistent use of PIAs will increase the awareness of privacy and data protection issues within the School and ensure that all relevant staff involved in designing projects think about privacy at its earliest stages.

Examples of where a PIA would be appropriate

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more schools seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new database which consolidates information held by separate parts of the school.
- Legislation, policy or strategies which will impact on privacy through the collection or use of information, or through surveillance or other monitoring.
- Cloud hosted applications.
- The collection of new data on an existing system.

7. PIA Procedure

The format for an initial PIA is at **Annex A.**

This review form is based on the eight Data Protection Principles described in Schedule 1 of the Data Protection Act.

In the event that a full PIA is deemed appropriate the format for this is at **Annex B**

The links between the PIA and DPA are set out in **Annex C**

8. Monitoring

The completed PIA should be submitted to the Governing Body for review and approval. The Governing Body will monitor implementation of actions identified in PIA's

(Extracted from the ICO – PIA Code of Practice)

Annex A

Privacy impact assessment screening questions

These questions are intended to help you decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

You can adapt these questions to develop a screening method that fits more closely with the types of project you are likely to assess.

- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
- Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.
- Will the project require you to contact individuals in ways that they may find intrusive?

(Extracted from the ICO – PIA Code of Practice)

Annex B

Privacy impact assessment template

This template is an example of how you can record the PIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a PIA. The template follows the process that is used in this code of practice. You can adapt the process and this template to produce something that allows your organisation to conduct effective PIAs integrated with your project management processes.

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the PIA process.

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Annex C can be used to help you identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns

(Extracted from the ICO – PIA Code of Practice)
Annex C

Linking the PIA to the data protection principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

- Have you identified the purpose of the project?
- How will you tell individuals about the use of their personal data?
- Do you need to amend your privacy notices?
- Have you established which conditions for processing apply?
- If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
- If your organisation is subject to the Human Rights Act, you also need to consider:
- Will your actions interfere with the right to privacy under Article 8?
- Have you identified the social need and aims of the project?
- Are your actions a proportionate response to the social need?

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

- Does your project plan cover all of the purposes for processing personal data?
- Have you identified potential new purposes as the scope of the project expands?

Principle 3

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

- Is the quality of the information good enough for the purposes it is used?
- Which personal data could you not use, without compromising the needs of the project?

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary? How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

- What retention periods are suitable for the personal data you will be processing?
- Are you procuring software that will allow you to delete information in line with your retention periods?

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

- Will the systems you are putting in place allow you to respond to subject access requests more easily?
- If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- Do any new systems provide protection against the security risks you have identified?

- What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

- Will the project require you to transfer data outside of the EEA?
- If you will be making transfers, how will you ensure that the data is adequately protected?
