Data Protection and Security Policy

Contents

APPROVAL DATE: 18 June 2018

REVIEW DATE: June 2019

1. About us

Welcome to Inspire!

We respect your right to privacy. This Data Protection and Security Policy sets out details of the information that we may collect from you and how we may use that information.

In this Data Protection and Security Policy, references to 'we' or 'us' are to 'Inspire! Education Business Partnership' and the 'Inspired Directions School', a company incorporated as 'New Hackney Education Business Partnership Limited' (registered number 05157521) whose registered office is at 34-38 Dalston Lane, London, England, E8 3AZ, who will be the controller of any personal data processed as described in this Data Protection and Security Policy.

All references to Inspire! throughout this policy refer to both Inspire! Education Business Partnership and the Inspired Directions School. The policy applies to both.

This policy meets the requirements of the GDPR and the expected provisions of the Data Protection Act 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR. We will put measures in place to show that we have integrated data protection into all of our data processing activities and demonstrate an approach of data protection by design and default.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Definitions

Term	Definition
Inspire!	All references to Inspire! throughout this policy will refer to both Inspire! Education Business Partnership and the Inspired Directions School.
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Sensitive personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions

	• Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

3. Data Protection principles

The GDPR is based on data protection principles which state that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

All information we collect is treated in line with these principles.

4. What information do we collect?

Inspire! holds personal data on staff, parents, pupils, governors, volunteers, service users and other individuals who come into contact with the organisation in order to deliver its

programmes and services. Inspire! is therefore a data controller and is registered as such with the ICO and will renew this registration as legally required.

If you are a young person who benefits from our programmes, we need to know your basic personal data to provide you appropriate updates and manage your applications. We also ask for sensitive personal information to monitor the diversity of young people on our programmes.

If you are a volunteer we need to know your basic personal data to provide you appropriate updates. We also ask for sensitive personal information to match you to the most appropriate events, and to ensure that our volunteers reflect the diversity of our local school population.

If you are an employer who works with Inspire! on any of our programmes, including the provision of work experience, we collect your basic information in order to manage our programmes, contact you to organise work experience, and provide you with appropriate updates.

If you are a pupil in the Inspired Directions School, we collect personal and sensitive information in line with school requirements.

If you are a trustee of Inspire! or a governor of the Inspired Directions School, we collect basic personal information for transparency reasons.

If you receive our newsletter we hold basic personal information on you in order to contact you. You can request to opt-out at any time by contacting us here: http://www.inspire-ebp.org.uk/contact-us.html

We will not collect any personal data from you that we do not need.

5. How do we use your information?

Inspire! is a data controller as both a charity and an alternative provision school. This means that we have numerous reasons for processing data.

We rely on the following legal bases for processing. These examples are not limited; there may be other areas where we use these bases for other functions.

We rely on 'legitimate interest' to process data associated with the sourcing, creation and matching of work experience placements. The processing justifies the impact on all individuals concerned: the employers, the schools, young people and Inspire! all have an interest in the creation of work experience placements which is in the public benefit. Information is stored on a password protected system and access is only given to relevant employees.

We have a legitimate interest to request student SEN information from schools for students who are part of our programmes designed to address their specific needs.

We also have a legitimate interest to contact individuals who have engaged with us in the past and hold a relationship with us. The nature of our work justifies our continued relationship with our stakeholders. The processing of data in relation to these examples is legitimate, necessary and balanced.

We rely on 'consent' to contact individuals about volunteering opportunities and be featured in photographs. Consent is clear, prominent, opt-in focused and necessary. Individuals can withdraw their consent at any time, and this policy explains how in paragraph 10.

We rely on 'contract' to process staff information, such as names and bank details, for their employment contracts. We also process information as part of our contractual obligations with London Borough of Hackney, and Service Level Agreements with schools, in order to run our programmes.

We rely on 'legal obligation' to carry out much of the processing in the Inspired Directions School in order to carry out its official functions. This includes information that we are legally obliged to collect for the school census and our communications with parents and guardians as part of our stature requirements as a school. For both the school and the charity, we are legally obliged to ensure that employees have no criminal convictions which bar them from working with children; we use pre-recruitment enhanced DBS checks to ensure this.

You can read about the six bases for processing data on the ICO's website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

6. How do we treat sensitive information?

We also process sensitive information, known under the GDPR as 'special category data', to carry out our activities.

We rely on 'explicit consent' to collect sensitive information from volunteers on some of our programmes. This is so we can plan events where the volunteers reflect school and community diversity.

We rely on 'legitimate activities' when we collect sensitive information from young people for programmes to monitor the diversity of our intake, and from schools to request SEN information on students part of our programme which are designed to address their specific needs. We couple this with explicit consent. We also rely on legitimate activities for the Inspired Directions School, an alternative provision school, to collect necessary information on students' needs.

We rely on 'medical' when collecting sensitive information from young people to determine if they have support needs that need to be provided for on our programmes. This is in line with our core activities of Inspire! and the Inspired Directions School.

You can read about special category data on the ICO's website here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

7. How is this information shared?

All the personal data we process is processed by our staff in the UK however for the purposes of IT hosting some of this information is located on international servers. Servers based outside of the EU are obliged to comply with GDPR regarding data that concerns EU citizens.

No third parties have access to your personal data unless the law allows them to do so. This may be in the cases as outlined below:

- If there is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- If we need to liaise with other agencies – we will seek consent as necessary before doing this
- If our suppliers or contractors need data to enable us to provide services to our staff and pupils. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

We will tell you what purposes we will use information for when we collect it and if information will be shared tell you why, with whom and under what circumstances.

We share personal information with others only when it is necessary and legally appropriate to do so. We have clear procedures for responding to requests for access to personal information (see section 10).

8. Who is responsible for this policy?

The Inspire! Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. Our DPO is Jacques Morris.

The DPO will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the organisation processes, and for the ICO.

The policy applies to **all staff** employed by Inspire!, and to external organisations or individuals working on our behalf.

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing Inspire! of any changes to their personal data, such as a change of address
- Contacting the Data Protection Officer (DPO) in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

All staff are provided with data protection training as part of their induction process.
Data protection will also form part of continuing professional development, where changes to legislation, guidance or Inspire!'s processes make it necessary.

9. How long do we keep information for?

We are committed to appropriate data retention and will ensure that information is not held longer than is necessary, and that when information is authorised for disposal it is done appropriately.

For example, we will keep volunteer information for as long as we run programmes that we feel will be of interest for you to return to as a volunteer. For those who receive our newsletter, we will retain your contact information for as long as we distribute a newsletter. For certain programmes we are contractually obliged to keep information for a number of years. After this period is complete, we delete your data.

We keep CCTV information for a period of one year and photograph information for as long as our programme and employment practices require.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Section 11 details our retention periods relating to HR and recruitment.

10. How can you manage or delete information about you?

You have the right to make a 'subject access request'. This may be to: confirm that we are processing your data; access a copy of your data; enquire why your data is being processed; enquire who the data has been, or will be, shared with; enquire how long the data will be stored for; or withdraw your consent, amongst other queries.

To submit a subject access request, write to the Data Protection Officer (DPO) using the details in section 21. Requests should include your name, contact details and details of your request. If staff receive a subject access request they should immediately forward it to the DPO. We will respond to requests using the procedure outlined in Appendix A.

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

11. How do we process recruitment and employment information?

All of the information you provide during the application process will only be used for the purpose of progressing your application, or to fulfil legal or regulatory requirements if necessary.

We will not share any of the information you provide during the recruitment process with any third parties for marketing purposes or store any of your information outside of the European Economic Area. The information you provide will be held securely by us and/or our data processors whether the information is in electronic or physical format.

We will use the contact details you provide to us to contact you to progress your application. The information we ask for is used to assess your suitability for employment. You don't have to provide what we ask for but it might affect your application if you don't.

Application stage

- We ask you for your personal details including name and contact details. We will also ask you about your previous experience, education, referees and for answers to questions relevant to the role you have applied for. At the application stage, or after a conditional offer of employment is made, you will be required to provide proof of your identity and qualifications. You will be asked to attend our office with original documents and we will take copies.
- You will also be asked for a criminal records declaration. This is only opened if a conditional offer of employment is made.
- You will also be asked to provide equal opportunities information. This is not mandatory information – if you don't provide it, it will not affect your application.

Conditional offer

- If we make a conditional offer of employment we will ask you for information so that we can carry out pre-employment checks. You must successfully complete pre-employment checks to progress to a final offer. We are required to confirm the identity of our staff, their right to work in the United Kingdom and seek assurance as to their trustworthiness, integrity and reliability.
- You will be asked to complete a criminal records declaration to declare any unspent convictions. We currently use GBG to manage this process for us. We require sight

of the documents that you use to complete your application in order to confirm details and upload them. We sometimes make copies of your documents if it is not possible to complete the process without doing so. Where we do, we immediately dispose of these copies after use. We do not retain copies of these documents. Our staff cannot view any personal documentation that you upload to GBG.

- We have a GDPR compliant contracts in place with our data processors, such as GBG. This means that they cannot do anything with your personal information unless we have instructed them to do it. They will not share your personal information with any organisation apart from us. They will hold it securely and retain it for the period we instruct.
- We will contact your referees, using the details you provide in your application, directly to obtain references.

If we make a final offer, we will also ask you for the following:

- Bank details – to process salary payments
- Emergency contact details – so we know who to contact in case you have an emergency at work

How long is the information retained for?

- If you are successful, the information you provide during the application process will be retained by us as part of your employee file for the duration of your employment plus 6 years following the end of your employment. This includes your criminal records declaration and references.
- If you are unsuccessful for the position you have applied for we will retain information provided as part of your application for a period of 12 months. We may also retain your information in our talent pool to proactively contact you should any further suitable vacancies arise during this period.

12. What other rights do you have with regards to your data?

In addition to the right to make a subject access request (see section 10), you also have the right to:

- Withdraw your consent to processing at any time
- Ask us to rectify, erase or restrict processing of your personal data, or object to the processing of it (in certain circumstances)
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which your personal data is transferred outside of the European Economic Area
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for your personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

13. CCTV, photographs and video

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded.

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Where we need consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer/pupil and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. We do not retain CCTV footage for a period longer than one year.

14. What are our security responsibilities?

We will:

1. ensure that access to confidential data is confined to those with justified authority to view it, with appropriate levels of access granted to users;
2. ensure that all system assets are operated according to specification;
3. ensure that information is only delivered to those who need it within the organisation, when appropriate, and is limited to these people;
4. ensure that databases have nominated users responsible for ensuring that the database is used in accordance with this policy;
5. encourage our partners to follow the principles outlined in this policy, and our IT support contractor will report incidents to Inspire! where necessary. Contractors will assist in monitoring the effectiveness of IT security within the organisation and initiating any requested changes to security procedures which become necessary as a result of the monitoring process; and
6. ensure the senior leadership team will ensure all IT systems in use are appropriately assessed for security compliance and are protected in accordance with this policy. Leadership will ensure that council employees using Inspire! systems are aware of their security responsibilities and receive awareness training.

15. How do we respond to security breaches and prevent harm?

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix B. When appropriate, we will report the data breach to the ICO within 72 hours.

Employees are trained in the reporting of security breaches and will use the form outlined in Appendix C to report breaches.

At the start of any new initiative, we will carry out a DPIA (Data Protection Impact Assessment) to ensure that we have considered any risks to the data we hold before making a change. We will demonstrate mitigation to any risks through the DPIA. Staff are trained on how to complete this, and it forms part of the project proposal process.

DPIAs will consider compliance risks, but also broader risks to the rights and freedoms of individuals. Our DPIA template is appended at Appendix D.

16. How do we manage secure access to our systems?

Inspire! employees will have access to machines only via usernames and passwords. The IT support management and IT Support contractor only have access to usernames and passwords. The Director will be responsible for resetting passwords and removing old data and information in the eventuality that equipment transfers between staff.

Project staff have additional password requirements specific to projects they are working on which will give them access to data and any sensitive project information. This access will be managed by line managers. Project passwords should not be shared with anyone without the clear and explicit permission of their project manager and for a specific reason – this includes not sharing access information with any non-project staff colleagues and volunteers.

The Director will ensure that usernames are locked in a timely manner when staff leave the organisation. The Director and Finance Manager will keep a record of user access rights for all staff across the organisation.

If necessary staff will follow the security breach process referred to in paragraph 13 and outlines in Appendix B.

17. How do we protect our hardware?

An asset register of computer equipment is maintained by Inspire! employees under whose responsibility the equipment is placed. No equipment should be removed from any site without the approval of line managers - except for portable computers / devices that are the responsibility of each named individual user. Hardware should not be left unattended, unless securely stored in lockable cabinets when not in use.

Hardware in particularly vulnerable areas or containing sensitive data should make use of physical security measures such as locking office doors or installing locking devices to secure hardware to desk. Redundant hardware (including PCs, laptops and portable devices) will be disposed of in accordance with the appropriate policies

Care should be exercised when eating or drinking near IT equipment. The location of all hardware (computers, printers, modems etc.) should comply with Health and Safety standards including the stability of the desk surface, and elimination of trailing cables.

All personal computers and printers should be switched off when not in use for extended periods, such as overnight or during weekends. Air vents on computers should not be obstructed

18. How do we control our software?

All software must be purchased through the central purchasing system and no software (including evaluation software) should be installed without prior permission from line managers. The download of files is not permitted unless agreed by line managers.

A register of software will be maintained centrally by the IT support provider. Software must not be copied, as this is an infringement of copyright and therefore illegal - unless specifically permitted by the licensing agreement. This includes loading the software from one set of disks onto several PCs

We ensure protection from viruses by following the Computer Misuse Act 1990 which states that the deliberate introduction of malicious software to a system is a criminal offence. No files should be loaded on to any system from an external portable device unless they have first been virus checked by staff. Anti-virus software is installed on Inspire! PCs and where a virus is detected this will be reported immediately to the IT support provider.

19. How do we keep our environment secure?

We ensure that security is carefully considered when locating PCs, using laptops on site and storing documents and paperwork. We ensure that all key holders responsible for lockable cabinets and doors will make the appropriate information security checks when opening / closing the office including closing down machines, ensuring cabinets are locked and areas containing sensitive information are secure. Appropriate signing in and signing out processes will be in place

20. How will we review this policy?

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect Inspire!'s practice. Otherwise, or from then on, this policy will be reviewed **annually** and shared with the full governing board.

Inspire! will notify you of changes to the Data Protection and Security Policy.

21. How can you contact Inspire!?

For further information on how your data is used, or if you have any questions, comments or complaints about this policy, please contact:

Jacques Morris
Data Protection Officer

020 7275 6060

Or write to us at:

FAO: Jacques Morris, Data Protection Officer
Inspire! Education Business Partnership
34-38 Dalston Lane
London
E8 3AZ

22. Appendix A: Subject access request procedure

This guidance is also available on the K Drive.

Individuals have the right to obtain confirmation that their data is being processed and access to their data, rectify their data or delete their data (erasure). This may be a written or verbal request.

All requests, verbal or written, should be recorded in the Subject Access Requests folder in the K drive.

Access: the requestor may obtain a copy of their data

Rectification: the requestor asks to have their data altered so it is accurate

Deletion (erasure): the requestor asks to have their data deleted

Quick guide:

Request	Cost	Timing	Record	Right to refuse?
Access	Free of charge (unless unfounded, excessive, repetitive)	Within one month (can be extended to 3)	K Drive	Yes, if unfounded, repetitive, excessive
Rectification	Free of charge (unless unfounded, excessive, repetitive)	Within one month (can be extended to 3)	K Drive	Yes, if unfounded, repetitive, excessive
Deletion (erasure)	Free of charge (unless unfounded, excessive, repetitive)	Within one month (can be extended to 3)	K Drive	Yes, if unfounded, repetitive, excessive

Use this checklist to respond to requests:

1. Does the information requested relate to the person requesting it? If you're not sure, request ID from the individual (but only ask for information you need to confirm their identity, nothing more).
2. Is the request legitimate? Is it unfounded, repetitive or excessive?
3. Do we have the appropriate contact information to respond?
4. Will we be able to respond within one month of receipt?
5. Can we provide the information in a commonly used electrical format?
6. If it is a large quantity of information being requested? If so, do we know exactly what information the requestor would like access to?

When does the right to erasure apply?

Individuals have the right to have their personal data erased if:

- The personal data is no longer necessary for the purpose which you originally collected or processed it for;

- You are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- You are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- You are processing the personal data for direct marketing purposes and the individual objects to that processing;
- You have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- You have to do it to comply with a legal obligation; or
- You have processed the personal data to offer information society services to a child.
- The request should be handled with particular weight if it comes from a child

When does the right to erasure not apply?

The right to erasure does not apply if processing is necessary for one of the following reasons:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation;
- For the performance of a task carried out in the public interest or in the exercise of official authority;
- For archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- For the establishment, exercise or defence of legal claims.
- The GDPR also specifies two circumstances where the right to erasure will not apply to special category data:
- If the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
- If the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health professional).

When requests are unfounded, repetitive or excessive

- We may refuse. Write to the requestor to explain the decision and inform them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.
- We may charge an appropriate fee

When requests are complex or numerous

- We may inform the requestor of an extension of a further two months to respond.

- We must explain why to the individual and inform them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

23. Appendix B: Security Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO, using the form in Appendix C.
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the director, head teacher and the chair of governors/ chair of trustees
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned

        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the K Drive.
- The DPO and Director will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

24. Appendix C: Security Breach Reporting Form

This form is also available on the K Drive

This form is to be used by a member of staff if an actual or suspected breach of data security has occurred.

The form should be completed by the individual employee who is responsible for the data in question or by their manager where appropriate and forwarded to the Data Protection Officer. The DPO will then use this report to inform their decision of whether to report the suspected breach or breach to the ICO.

Description of breach or suspected breach – what actually happened:

Description of data lost or potentially lost (please specify)

Agreed action(s)

Confirm when action(s) have been taken and outline any changes that will be put in place to avoid similar occurrence in future.

Signed (individual who was responsible for data)

_____

Line manager

_____

Date

_____

This incident report should be retained on site for audit reasons.

25. Appendix D: DPIA Template

This form and accompanying guidance is also available on the K Drive

1. The need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. If you're completing a business case/ project proposal you should append this DPIA to the case. *Summarise why you identified the need for a DPIA.*

2. Project objectives

What are the objectives of your project and why do you need to process data?

3. Describe the processing

How will you collect, use and store data? *Will you share the data?* *What is the high risk?* *How much data is there, and does it include sensitive and/or criminal information?* *How long will you keep the data?* *How many individuals are affected?* *What geographical area does it cover?* *What control will individuals have over their data? Are you using technology to ensure the data is accessible to individuals?*

4. Describe the storage and access

Who will have access and how will you store it securely?

5. Consultation process

Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

6. Necessity and proportionality

What is your lawful basis for processing? *Does the processing actually achieve your purpose? Is there another way to achieve the same outcome?* *How will you ensure data quality and data minimisation?* *What information will you give individuals?* *How will you help to support their rights?* *What measures do you take to ensure processors comply?*

7. Risk mitigation

Description	Risk	Mitigation	Likelihood	Severity
			H/M/L	*H/M/L*
			H/M/L	*H/M/L*
			H/M/L	*H/M/L*

8. Sign off

Note: if this DPIA indicates that the processing would result in a high risk and you are unable to mitigate those risks by reasonable means, you should contact the ICO to seek their opinion as to whether the processing operation complies with the GDPR: https://ico.org.uk/global/contact-us/

Author [Senior Programme Manager]:

Approval of DPO (yes/no):

Date:

DPO advice (on risks, implementation, changes etc):

This DPIA will be kept under review by: