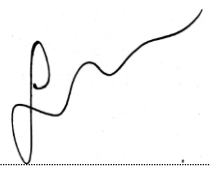
Higham Lane School
Helping Learners Succeed

Data Protection Policy

Policy Number	**59**
Approval Date	**July 2025**
Review Date	**July 2026**
Governors' Sub-Committee	**Resources & Premises**
Statutory Policy	**Yes**

Signed:  **Chair of Governors** Date: **July 2025**

Contents

1. Aims

Higham Lane School aims to ensure that all personal data collected about staff, students, parents/carers, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

The School recognises data protection is more than just a legal compliance. We recognise that respecting the confidentiality of personal data is critical to preserving the trust of our staff, students, parents/carers, governors, visitors and other individuals for building the foundations for a strong relationship with all in the School's community and beyond. Through developing systems for the protection and security of data, the School is making a commitment to treat all personal data with care and respect.

This policy and any other documents referred to in it set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

This policy does not form part of any employee's contract of employment and may be amended at any time.

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

2. Legislation and guidance

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

3. The data controller

Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities as a school, we will collect, store and process personal data about our staff, students, parents/carers, governors, volunteers, visitors and others. This makes us a data controller in relation to that personal data.

The School is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

4. Roles and responsibilities

The School expects that everyone working within the School, whether as an employee, volunteer or contractor ,must recognise their role in ensuring the safety of personal data and their requirement to follow the policies and procedures set out for the protection of personal data in the School.

Staff who do not comply with this policy may face disciplinary action.

4.1 Governing Board

The governing board has overall responsibility for ensuring that the School complies with all relevant data protection obligations.

4.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for providing advice and guidance to the School in order to assist the School to implement this policy, monitor compliance with data protection law, and develop related policies and guidelines where applicable.

The DPO will carry out an annual audit of the School's data processing activities and report to the Governing Board their advice and recommendations on school data protection issues.

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

Our DPO is the School DPO Service and is contactable via schooldpo@warwickshire.gov.uk or alternatively;

School Data Protection Officer
Warwickshire Legal Services
Warwickshire County Council
Shire Hall
Market Square
Warwick
CV34 4RL

4.3 Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis.

4.4 Assistant Headteacher and Director of Corporate Services

The School has nominated the following individuals as designated persons to be contacted internally in relation to all matters relating to data protection issues, and to make referrals, where necessary, to the Data Protection Officer.
Ian Naisbitt (Assistant Headteacher) who is contactable via dpo@highamlaneschool.co.uk
Ben Elliott (Director of Corporate Services) who is contactable via dpo@highamlaneschool.co.uk
Data Protection Officer
Higham Lane School
Shanklin Drive
Nuneaton
CV10 0BJ
Tel: 02476 388123

4.5 All staff

All members of staff must be aware of their duties and responsibilities towards the protection of personal data and adhering to this policy. Any breach of this policy may result in disciplinary or other action. Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the School's designated Data Protection Lead 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

5. Data Protection Principles – Fair and lawful processing

The GDPR is based on data protection principles that the School must comply with. Higham Lane School has adopted the principles to underpin its Data Protection Policy:

The principles require that all personal data shall be:

(1) processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');
(2) used for specified, explicit and legitimate purposes ('purpose limitation');
(3) used in a way that is adequate, relevant and limited to what is necessary ('data minimisation');
(4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, are erased or rectified without delay ('accuracy');
(5) kept no longer than is necessary ('storage limitation');
(6) processed in a manner that ensures it is safe and secure, ensuring that measures against unauthorised or unlawful processing and against accidental loss, destruction or damage are in place ('integrity and confidentiality').

This policy sets out how the School aims to comply with these principles.

Data Protection legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For personal data to be processed fairly, data subjects must be made aware:

- that the personal data is being processed
- why the personal data is being processed
- what the lawful basis is for that processing (see below)
- whether the personal data will be shared, and if so with whom
- the period for which the personal data will be held
- the existence of the data subject's rights in relation to the processing of that personal data
- the right of the data subject to raise a complaint with the ICO in relation to any processing.

We will only obtain such personal data as is necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any processing.

6. Collecting personal data

6.1 Lawfulness, fairness and transparency

Higham Lane School shall only process personal data where it has one of 5 'lawful bases' (legal reasons) available to the School to do so under data protection law:

- The data needs to be processed so that the School can **fulfil a contract** with the individual, or the individual has asked the School to take specific steps before entering into a contract
- The data needs to be processed so that the School can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the School, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the student is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

6.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

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.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with guidance set out in the Information and Records Management Society's Toolkit for Schools.

7. Sharing personal data

We will not normally share personal data with anyone else except as set out in the School's Privacy Notice. The GDPR and the DPA 2018 also allow information to be shared where:

- There is an issue with a student or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. 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 Her majesty's Revenue and Customs (HMRC)

- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations (Please refer to our Safeguarding Policy)
- 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 students or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

8. Subject access requests and other rights of individuals

8.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the Data Protection Officer. They should include:

- Name of individual
- Name of School
- Correspondence address
- Contact number and email address
- Details of the information requested

The DPO will send the subject access request to the School's designated Data Protection Lead. If staff receive a subject access request, they must immediately forward it to the designated School Data Protection Lead, who will ensure that the DPO is informed.

Information to be released will be collated by the School and then sent to the DPO for checking and sending out to the applicant.

8.2 Children and subject access requests

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 person should have parental responsibility for the child, and the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from those with parental responsibility for students at our school aged 13 and above may not be granted without the express permission of the student.

Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from those with parental responsibility for students at our school [aged under 13] will in general be granted without requiring the express permission of the student.

8.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous, or where it is impractical to comply within a month due to school closure. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

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

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

8.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time, where processing is based on the consent of the student or parent
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- 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 their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the School's designated Data Protection Lead who will send it to the DPO for information purposes.

9. Parental/carer requests to see the educational record

Any requests from parents/carers should be treated as subject access requests in accordance with the above.

10. Biometric recognition systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The School will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use the School's biometric system(s). We will provide alternative means of accessing the relevant services for those students. Parents/carers and students can object to participation in the School's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

Where staff members or other adults use the School's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the School will delete any relevant data already captured.

11. Closed-Circuit Television (CCTV)

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. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to dpo@highamlaneschool.co.uk

12. Photographs and videos

As a school we want to celebrate the achievements of our students and therefore may want to use images and videos of our students within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. The School will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where the School need parental consent, it shall clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where the School doesn't need parental consent, it shall clearly explain to the student how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school newsletters, etc.
- Outside of school by external agencies such as the school photographer and newspapers
- Online on our school website or social media pages

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.

When using photographs and videos in this way, we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Please see our Safeguarding Policy and Privacy Notice for more information on our use of photographs and videos.

13. Data protection by design and default

The School shall put measures in place to show that it has integrated data protection into all of its data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the School's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

The School will protect personal data and take appropriate security measures against unlawful or unauthorised processing, alteration and disclosure of personal data, and against the accidental loss of, or damage to, personal data.

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. All data will be held and disposed of in line with the School's Data Retention and Destruction Policy.

In particular:

- Entry controls:
  - Appropriate building security measures such as alarms, window bars and deadlocks
  - Visitors are required to sign in and out and are, where appropriate, accompanied
  - Any stranger seen in entry-controlled areas should be reported immediately to the most senior member of staff on site at the time
- Secure lockable desks and cupboards - Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- Methods of disposal - Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the ICO guidance on the disposal of IT assets. https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations. pdf
- Equipment - Data users must ensure that individual monitors and projector screens do not show confidential information to passers-by and that they lock access to their screen or log off from their PC when it is left unattended.
- Handling telephone calls or responding to emails - Staff must ensure they check the requestor's identify before providing or confirming any personal information to the caller or responding to an email.
- Postal Services - Where it is necessary to send personal information by post staff should consider sending personal data by registered mail. Staff should take every opportunity to verify the current address of the recipient to ensure information is sent to the correct address.
- Internal mail or student post - Care should be taken not to send sensitive or personal data home with a student or through an internal mail system.
- Clear desk policy - The Schools promotes a clear desk policy. Documents should not be left on desks or work spaces overnight. This includes data printouts but also extends to handwritten notebook pages and notes which can contain confidential data too. Staff should clear their desks and lock any information away which may contain confidential data.
- Working away from the school premises – paper documents. Staff are discouraged from taking paper records containing personal data away from the School office. Where this is absolutely necessary paper records and files containing personal data should be handled in such a way as to restrict access only to those with a legitimate reason to access them. This includes securely storing or locking personal data way when not required.
- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

The School will ensure that IT systems are set up so that the access to protected files is denied for unauthorised users and that users will be assigned clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

- All users will use strong passwords, incorporating numbers and mixed case, which must be changed regularly. User passwords must never be shared.
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes or less.
- Standard unencrypted email should never be used to transmit personal or sensitive data. Only school email accounts should be used to transmit such data. Staff should <u>never</u> use personal email accounts to receive or send personal data.
- Staff should take care to ensure any emails containing personal data are sent only to the intended recipient and avoid including recipients unnecessarily. Caution should be used when selecting the *'Reply To All'* option.

- Where accessing data remotely this must be done via a secure encrypted link with relevant access controls in place.
- Personal data can only be stored on school equipment (this includes computers and portable devices such as laptops). Private equipment (i.e. owned by the users) must not be used for the storage of personal data.
- The servers and IT infrastructure which forms part of the IT network will be kept in locked rooms and cabinets. Only qualified IT employees or suitably appointed IT contractors may access the physical servers and infrastructure.
- When personal data is stored on any portable computer system:
  - the data must be encrypted and password protected
  - the device must be encrypted and password protected
  - the device must offer approved virus and malware checking software
  - the data must be securely deleted from the device once it has been transferred or its use is complete.
- The use of memory cards, USB memory sticks or other portable storage devices are forbidden. Staff are encouraged to access data remotely through the School's remote desktop facility.
- The School have clear policies and procedures for the automatic backing up, accessing and restoring all data held on the School's systems, including off-site backups.

Cloud based storage systems - Where the School has cloud based storage systems it will:

- Ensure it carries out the appropriate due diligence, including enquiring into the location of the relevant IT servers.
- Is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection legislation
- Ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.(see the ICO advice on cloud based storage - http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx)
- Inform the DPO of the use of Cloud based storage systems and the security procedures in place prior to entering into an agreement with the supplier

Document printing - Documents containing personal data must be collected immediately from printers and not left on photocopiers.

Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

15. Data Protection Impact Assessments (DPIA)

The School takes data protection very seriously, and will consider and comply with the requirements of Data Protection legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

In certain circumstances, the law requires us to carry out detailed assessments of proposed processing. This includes where we intend to use new technologies which might pose a high risk to the rights of data subjects because of the types of data we will be processing or the way that we intend to do so.

The School will complete an assessment of any such proposed processing and has a template document which ensures that all relevant matters are considered.

The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, the School will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the School's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

The School shall take all reasonable steps to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, the School shall report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of students eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about students

18. Remote Education and GDPR (Data Protection, Information Security and Online Safety)

When engaging a third-party data processor to provide us with a platform to deliver remote education, Higham Lane School will:

- Ensure the service provides sufficient guarantees of their GDPR compliance.
- Share only information that is considered necessary for the system to work and operate in order to achieve the required purpose.
- Conduct a Data Protection Impact Assessment to identify and minimise risk.
- Inform individuals of the details of any third-party processor and the data to be processed for these purposes by updating your privacy notices.

When staff are required to work from home in order to deliver education, Higham Lane School shall:

- Provide staff with a secure, school registered device to work from.
- Ensure staff are briefed and familiar with the school's remote working policy.
- Ensure all staff are up to date with data protection training.

When implementing a platform where students are required to engage in online activities, Higham Lane School will:

- Ensure parents are informed of the type of work children are being asked to do.
- Provide information on who is likely to engage with pupils online in order to deliver online teaching.
- Share information and guidance with parents to ensure they are able to effectively monitor their children's safety online.
- Review settings to ensure they are set to the most secure and practical format that is possible.
- Review privacy settings of all platforms used for online teaching (e.g. GSuite, Google Classroom) to ensure children are not placed at risk.

- If uploading information to an open cloud-based system, we will ensure no personal information that identifies individuals is included.
- Take all reasonable steps to ensure that risks of harm to children through inappropriate access via online portals are reduced as far as possible.
- Continuously liaise with our safeguarding team to ensure we are following all relevant safeguarding guidance.

19. Training

All staff and governors 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 the school's processes make it necessary.

20. Links with other policies

This Data Protection Policy is linked to our:

- Information Security Policy
- Security Incidents and Breach Reporting Policy
- ICT and Acceptable Use Policy
- Safeguarding Policy
- Privacy Notices

21. Changes to this policy

We may change this policy at any time. Where appropriate, we will notify data subjects of those changes.

Appendix 1: Personal data breach procedures

If staff become aware that information has not been handled according to procedures and there is a data breach or potential security incident, they must report it in accordance with this procedure.

When appropriate, the School will report the data breach to the ICO within 72 hours in accordance with the requirements of the GDPR.

1. Data protection breaches occur where personal data is lost, damaged, destroyed, stolen, misused and/or accessed unlawfully.

2. Examples of how a breach may occur include:

    a. Theft of data or equipment on which data is stored;
    b. Loss of data or equipment on which data is stored;
    c. Inappropriate access controls allowing unauthorised use;
    d. Accidental Loss;
    e. Destruction of personal data;
    f. Damage to personal data;
    g. Equipment failure;
    h. Unlawful disclosure of personal data to a third party;
    i. Human error;
    j. Unforeseen circumstances such as fire or flood;
    k. Hacking attack; or
    l. 'Blagging' offences where information is obtained by deceiving the organisation which holds it.

3. If any member of staff of the School, or a governor discovers that data has been lost, or believes that there has been a breach of the data protection principles in the way that data is handled, they must immediately or no later than within 24 hours of first coming to notice, inform the School's designated Data Protection Lead.

4. Upon being notified, the School's designated Data Protection Lead will assess whether a breach of personal information has occurred, and the level of severity. If a breach has occurred but the risk of harm to any individual is low (for example, because no personal information has left the control of the School, then the School's Data Protection Lead will undertake an internal investigation to consider whether the Information Security Policy was followed, and whether any alterations need to be made to internal procedures as a result.

5. In all other cases, the incident must be notified to the Data Protection Officer immediately, who must follow the Information Commissioner's Office guidelines on notification and recording of the breach. The priority must then be to close or contain the breach to mitigate / minimise the risks to those individuals affected by it.

All School staff and Governors are expected to work in partnership with the designated Data Protection Lead and the Data Protection Officer in relation to the following matters.

Notification of Breaches

Any member of staff or Governor who becomes aware of a personal information breach should provide full details to the designated Data Protection Lead for the School within 24 hours of being made aware of the breach. The Data Protection Lead will then complete the Data Breach Record Form and Incident Log. When completing the form, details should be provided of the reporter's name, the date/time of the breach, the date/time of detecting the breach, and basic information about the type of breach and information about personal data concerned. Details of what has already been done to respond to the risks posed by the breach should also be included.

Containment and Recovery

The initial response is to investigate and contain the situation and a recovery plan including damage limitation. The School may need input from specialists such as IT, HR and legal and in some cases contact with external third parties.

The School should:

- Seek assistance in the containment exercise. This could be isolating or closing a compromised section of the network, recovery of released documents, finding a lost piece of equipment or simply changing any related access codes
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause.
- As well as the physical recovery of equipment, this could involve the use of backup records to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Consider whether any individual affected by the data breach should be notified

Assessing the Risks

Levels of risk can be very different and vary on an individual breach of data security depending what is lost/damaged/stolen. For example, if a case file is lost then risks are different depending on type of data and its sensitivity with potential adverse consequences for individuals. The designated Data Protection Lead should consider the following points:

- What type of data is involved?
- How sensitive is the data?
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data?
- If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate? If it has been damaged, this poses a different type and level of risk.
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
- How many individuals' personal data has been affected by the breach?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals?
- Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to life?
- Loss of public confidence in the School?

All staff and Governors establish whether there is anything they can do to recover any losses and limit the damage the breach can cause.

Appendix 2: Personal data breach log and incident reporting form

Personal Data Security Breach Log

Organisation: Higham Lane School

NO.	REF.	DETAILS OF THE BREACH						CONSEQUENCES OF BREACH	MEASURES TAKEN/ TO BE TAKEN?			
		Date/time of incident	No. of people whose data is affected	Nature of breach	Description of how breach occurred	How did you become aware of the breach/When was breach reported to you?	Description of personal data involved		What remedial action was taken?	Have the affected data subjects been informed?	Has the DPO been informed?	Does the breach need to be reported to the ICO?

Personal Data Security Breach – Incident Reporting Form

This form should be used to provide information to the Data Protection Officer when there has been a *serious* breach and consideration needs to be given to whether the breach should be reported to the ICO.

The aim of the form is to gather detailed information in order to understand the gravity of the breach, including its impact and what must be done to reduce the risk to personal data and the individuals concerned.

It is imperative that as much information as possible is provided.

The information will be used to review policies and procedures and assess whether changes are required.

Breach log no: _____

Breach log reference: _____

1. Details of the breach

a) Date and Time of the Incident

b) Number and description of individuals whose data is affected (eg 3 year 10 pupils)

c) Department (if relevant)

Appendix 3: Definitions

Term	Definition
Data	Is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	For the purpose of this policy include all living individuals about whom we hold personal data. This includes students 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	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
Special Category Personal Data	Includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data
Data audit / data asset register	The assessment of data and its quality, for a specific purpose. A list of personal data assets that the academy holds
Lawful basis and conditions for processing	There are specific reasons, set out in law, for which you can process personal data and another list for processing special category data
Data Retention	How long personal data can be held for. At the end of the data retention period set out in the Data Retention and Destruction Policy processes should be in place to ensure the data is securely disposed of.
Subject Access Request (SAR)	Where a person (data subject) requests access to the information held about them. See the Subject Access Request Policy for further information on legal timescale and procedures for dealing with SAR's
Data Protection Impact Assessment (DPIA)	The process to consider the implications of changes to systems and procedures which impact on the privacy of individuals. Assessing privacy at the outset helps you plan effectively and ensure your systems have 'privacy by design' at their heart
Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, This includes breaches that are both accidental and deliberate.

Data Controllers	Are the people who or organisations which 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 Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	Are those of our staff (including governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	Includes any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	Is any activity that involves use of the 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
Automated decision making / profiling	When software applies rules to data and makes a determination about a person based purely on the rules applied. For example if a person with 99% attendance automatically receives a reward.