Data Protection Policy

GLEBE HOUSE
SCHOOL & NURSERY
HUNSTANTON

This policy was updated in September 2025.
Review is due for the beginning of September 2026.
All changes from previous documents and sections have been highlighted yellow.

Contents

This policy initiated - September 2024
Policy written by - The Head and Bursar
Policy to be updated on an annual basis.
(Delete if not applicable) ***This policy is currently under review***

Change Log – for 2025/2026

Sections which have changes from the previous Data Protection Policy

The policy is currently under full review - September 2025

Aims

Glebe House School Trust in this policy are referred to as “we”, “us” or Glebe House School and Nursery (“the School”). We aim to ensure that all personal data collected about staff, pupils, parents, governors, contractors, volunteers, visitors, and other individuals is collected, stored, and processed in accordance with current data protection legislation. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

This Notice applies to the whole School, including the EYFS.

Legislation and Guidance

This policy meets the requirements of the UK General Data Protection Regulations (GDPR), Data Protection Act 2018 and the Freedom of Information Act 2000. It is based on guidance published by the Information Commissioner’s Office (ICO) on the GDPR, the ICO’s code of practice for subject access requests and IT asset disposal for organisations.

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

Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. For example: ● Name (including initials) ● Home address, contact details ● Pupil records ● Photos and videos ● Personal data may exist as an electronic record and as a hard copy (pap otherwise)
Special Categories of Personal Data	Personal data which is more sensitive and so needs more protection. For examp ● Religious beliefs ● Ethnicity ● Sexual orientation ● Medical history ● Special Educational Needs ● Biometric data
Processing	● Anything done to personal data, such as collecting, recording, organising structuring, storing, adapting, altering, retrieving, using, disseminating, er or destroying and sharing. ● 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, wh processes personal data on behalf of the data controller.
Personal Data Breach	● A breach of security leading to the accidental or unlawful destruction, los alteration, unauthorised disclosure of, or access to personal data.
Third Party	● Any external organization with whom personal data is shared.

The Data Controller

The School processes personal data relating to parents, pupils, staff, governors, contractors, volunteers, visitors and others, and therefore is a Data Controller. The DFO has responsibility as the Privacy Officer on behalf of the School.

Roles and Responsibilities

This policy applies to all staff employed by the School, and to external organisations, contractors or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing Board

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

Primary Data Controller

The Privacy Officer is responsible for:

- Overseeing the implementation of this policy
- Informing and advising members of staff regarding their obligations to comply with UK GDPR and other related data protection legislation and guidance
- Monitoring our compliance with data protection law
- Developing related policies and guidelines where applicable
- Acting as the first point of contact for the ICO and for individuals whose data is being processed
- Coordinating a proactive and preventative approach to data protection.
- Calculating and evaluating the risks associated with the school's data processing.
- Having regard to the nature, scope, context, and purposes of all data processing.
- Prioritising and focussing on more risky activities, e.g. where special category data is being
- processed.
- Promoting a culture of privacy awareness throughout the school community.
- Carrying out ad hoc reviews of data practices to ensure staff understand and are acting in accordance with relevant data protection laws.
- The DFO fulfills this responsibility on a day-to-day basis.

At Glebe House School and Nursery, the Primary Data Controller is the **Head - Adrian Stewart**

All staff

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 Privacy Officer 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 believe *any* personal data is inaccurate or untrue or have concerns as to how the data is recorded or processed
- If they wish to share personal data with third parties
- 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

Data Protection Principles

The School seeks to address (amongst other things) the following key regulatory principles within this policy:

- Lawfulness, fairness and transparency in the handling and use of personal data. The School will ensure that we make it clear how we are using personal data, on which “lawful bases” we are processing the information and that we recognise and uphold the rights of the Data Subjects.
- Limiting the processing of personal data to specified, explicit, and legitimate purposes. The School shall not use personal data for purposes that are “incompatible” with the purpose for which the data was originally collected.
- Minimising the collection and storage of personal data so that we only collect and retain what is adequate, relevant and limited for the intended purpose of processing.
- Ensuring the accuracy of personal data, and where necessary keeping it up to date, and enabling it to be erased or rectified without delay.
- Limiting the storage of personal data. The School will ensure that we retain personal data only as long as necessary to achieve the purposes for which it was collected.
- Ensuring security, integrity, and confidentiality of personal data. The School employs appropriate technical and organisational security measures to keep personal data secure.

The UK GDPR's broader 'accountability' principle

Also requires that the School not only processes personal data in a fair and legal manner but that we are also able to demonstrate that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments (“DPIA”)); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters.

Collecting Personal Data

Processing

The School processes information in order to fulfill our contractual obligations to provide educational services, safeguard and promote the welfare of its pupils, promote the objects and interests of the School, facilitate the efficient operation of the School, and ensure that all relevant legal obligations of the School are complied with.

The School may process different types of information about staff, pupils, parents, governors, contractors, volunteers, visitors, and other individuals for the purposes set out above. That information may include (but is not limited to):

- Personal details such as home address, contact details, date of birth and next of kin
- Identification documents
- Pupils’ performance at School, including assessments, reports, examination reports, discipline record, attendance information
- Special educational needs
- Medical records and information, including details of any illnesses, allergies or other medical conditions suffered by a pupil

- Safeguarding information
- Details of any support received, including learning support, therapists, counselling, care plans and support providers
- Sensitive personal data such as religious beliefs
- Images of pupils and staff (and occasionally other individuals) engaging in School activities
- Bank details and National Insurance Number
- Performance Development Records
- CCTV images for security purposes

Lawfulness, Fairness and Transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do sounder data protection law:

- The data needs to be processed so that the School can fulfil a contract with the individual, or to enter 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 for the legitimate interests of the School or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/guardian when appropriate in the case of a pupil) 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).

Whenever we initially collect personal data directly from individuals, we will provide them with the relevant information required by data protection law in the form of a Privacy Notice to include:

- Notice that the personal data is being processed.
- Why the personal data is being processed.
- What the lawful basis is for that processing.
- Whether the personal data will be shared, and if so, with whom.
- 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.

The privacy notices supplied to individuals, including pupils, in regard to the processing of their personal data will be written in clear, plain, age-appropriate language which is concise, transparent, easily accessible and free of charge.

Personal data (including sensitive personal data, where appropriate) is processed by the School inorder to:

- administer admissions
- support pupils' teaching and learning;
- monitor and report on pupil progress;
- provide appropriate pastoral care and safeguarding
- communicate with individuals with links to the School
- where appropriate, promote the School to prospective pupils (including through the School's prospectus, website and social media applications);
- other reasonable purposes relating to the operation of the School including to obtain appropriate professional advice and insurance for the School.
- carry out obligations under employment, social security or social protection law, or a collective agreement

- process payroll
- Support members of staff in respect of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis or the provision of health or social care
- facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- support effective performance management and inform our recruitment and retention policies
- allow better financial modelling and planning

Limitation, Minimisation and Accuracy

We will only collect personal data for specified, explicit and legitimate reasons. 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.

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 the School's Data Protection – Good Practice Guidelines.

Consent

Consent must be a positive indication expressly confirmed in words. It cannot be inferred from silence, inactivity, a positive action without words or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Consent can be withdrawn by the individual at any time.

The school ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Where the school opts to provide an online service directly to a pupil, the pupil is aged 13 or over, and the consent meets the requirements outlined above, the school obtains consent directly from that pupil; otherwise, consent is obtained from whoever holds parental responsibility for the pupil, except where the processing is related to preventative or counseling services offered directly to pupils. In all other instances with regard to obtaining consent, an appropriate age of consent is considered by the school on a case-by-case basis, taking into account the requirements outlined above.

Sharing Personal Data

During the course of our daily activities the School will frequently engage with third-party organisations and may need to share personal data with them. A list of the third parties, with whom the School regularly shares data is available on request. The individuals concerned will be informed when the School shares personal data with third parties not on this list. The School will seek to ensure any third party upholds the principles of Data Protection as laid out in this document.

Personal data may be shared with a third party where:

- there is an issue with a pupil or parent/guardian that puts the safety of a pupil or our staff at risk
- we need to liaise with other agencies
- to enable the relevant authorities to monitor the School's performance i.e. IndependentSchools Inspectorate;
- to compile statistical information (normally used on an anonymous basis);
- to safeguard pupils' welfare and provide appropriate pastoral (and where relevant, medical and dental) care for pupils;

- where specifically requested by pupils and/or their parents or guardians;
- to enable pupils to take part in national and other assessments and to monitor pupils' progress and educational needs;
- where necessary in connection with learning and extra-curricular activities undertaken by pupils e.g. educational visits, peripatetic teachers, residential trip providers, extra- curricular providers;
- to obtain appropriate professional advice
- where a reference or other information about a pupil or ex-pupil is requested by another educational establishment or employer to whom they have applied;
- in support of our marketing activities;
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT support.
- the use by the School of online academic and educational services
- the use by the School of cloud IT services such as delivery of remote learning, email and file storage for staff and pupils

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 only transfer personal data to a country or territory outside the European Economic Area if we are satisfied the third party(s) involved will only process the data in accordance with data protection law.

The school understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

Subject Access Requests and Other Rights of Individuals

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

The School is not required to disclose any pupil examination scripts (or other information consisting solely of pupil test answers, potentially including in mock exam scripts or other types of exams / tests used to assess performance). The School is also not required to provide examination or other test marks ahead of their ordinary publication date, nor share any confidential reference held by the School that was (or will be) given for the purposes of the education, training, appointment or employment of any individual.

Subject Access Requests must be submitted in writing, either by letter or, email privacy@crosfields.com to the Privacy Officer. They should include:

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

Children and Subject Access Requests

Personal data about a pupil belongs to that pupil, and not the pupils' parents or guardians. For a parent or guardian 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.

Pupils 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, most Subject Access Requests from parents or guardians of pupils at the School may be granted without the express permission of the pupil. Children aged 13 and above may be mature enough to understand their rights and the implications of a Subject Access Request and therefore, a Subject Access Request from parents or guardians may require additional permission from the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to Subject Access Requests

When responding to requests, we:

- Will take appropriate steps to confirm the identity of the person making the request
    - 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. Should the corresponding date in the following month fall on a weekend or public holiday, the final date will be the next working day.
- 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. We will inform the individual of this within 1 month, and explain why the extension is necessary and that they may seek redress with the Information Commissioner's Office if they feel this extension is not warranted

We will not disclose information if it:

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

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. For example, repetitive requests or ones which ask for further copies of the same information would be regarded as unfounded or excessive.

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

The school will ensure that information released in response to a Subject Access Request does not disclose personal data of another individual. If responding to the Subject Access Request in the usual way would disclose such data, the school will:

- Omit or redact certain elements from the response if another individual's personal data would be disclosed otherwise.
- Reject requests that cannot be fulfilled without disclosing another individual's personal data, unless that individual consents or it is reasonable to comply without consent.
- Explain to the individual who made the Subject Access Request why their request could not be responded to in full.
- In the event that a large quantity of information needs to be processed about an individual, the school will ask the individual to be as specific as possible about the information requested – the time limit for responding to the request will be paused until clarification from the individual is received.

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 (see section 7), individuals also have the right to:

- Request rectification of any data that is inaccurate or incomplete
- Have their personal data erased and to prevent further processing if:
- It is no longer required for the purposes for which it was collected
- Consent is withdrawn
- There is an opposition to the processing and no superseding legitimate interest
- The personal data is being unlawfully processed
- The personal data must be removed in order to comply with a legal obligation
- Request a restriction of further processing of personal data
- Object to processing on specific grounds
- Obtain and reuse their personal data for their own purposes across different services.

Individuals should submit any request to exercise these rights to the DFO. If staff receive such a request, they must immediately forward it to the DFO.

Where it is not possible to comply with such requests, the data subject will be informed of the reason(s).

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 the Head of Estates.

Photographs and Videos

As part of the School activities, we may take photographs and record images of individuals within the School.

We will obtain written consent from parents/guardians for photographs and videos to be taken of their child and from staff for communication, marketing, and promotional materials on enrolment and at intervals not exceeding three years thereafter on an annual basis.

Uses may include:

- Within School on notice boards and in School magazines, brochures, newsletters, etc.
- Outside of School by external agencies such as the School photographer, prospectus, newspapers, campaigns
- Online on the School website, intranet or social media pages including Facebook, X (formerly Twitter),Instagram and Flickr.

Consent can be withdrawn at any time. If consent is withdrawn, we will delete the photograph or video from all locations 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 pupil, to ensure they cannot be identified, unless specific consent is provided.

See our Photography Policy for more information on our use of photographs and videos.

We may also record “Teams” sessions for safeguarding and record-keeping purposes. These files will not be used for any promotional purposes and will be removed after 28 days.

Biometric Information

We may wish to use biometric information about members of staff, Senior School pupils and regular visitors as part of an automated biometric recognition system. Biometric information is information about a person's physical or behavioural characteristics that can be used to identify him/her. We will use fingerprints for security/access control and payment systems.

We will notify each parent of the pupil and obtain the written consent of at least one parent and the pupil (Senior School only) before we can use that pupil's biometric information. Members of staff and regular visitors will also have to provide written consent for the use of their biometric information. We will provide a separate biometric information notice.
The law places specific requirements on the School when it uses biometric information. For example:

- We cannot use the information for any purposes other than those described above;
- We must ensure that the information is stored securely;
- We must tell those people for whom we hold biometric information, what we intend to do with the information;
- We will not disclose the biometric information to a third party unless permitted by law. We may however share the information with Suprema Inc. and Kappture (Advanced IT Ltd) for the proper use of the automated biometric recognition system.

Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- 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)
- Considering data protection issues as part of the design and implementation of systems, services and practices.
- Making data protection an essential component of the core functionality of processing systems and services.
- Automatically protecting personal data in school ICT systems.
- Implementing technical measures within the school network and ICT systems to ensure data is kept secure.
- Ensuring that documents are written in plain language so individuals can easily understand what is being done with personal data.
- Completing Data Protection 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
- Integrating data protection guidance and policy into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep records 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 theSchool 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

Data Protection Impact Assessments

DPIAs will be used in certain circumstances to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy. DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals, and will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV or biometric data.

The school will ensure that all DPIAs include the following information:

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

Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Paper-based records that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access
- Passwords that are at least 8 characters long containing letters, special characters and numbers are used to access School computers and laptops.
- Personal information may only be stored on School devices or within an @glebehouseschool.co.uk Google Account. Staff and governors may access cloud-based services from their personal devices and are expected to follow the same security procedures as for School-owned equipment.
- 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 (see section 8)

Disposal of Records

While also complying with our Records Retention Policy, 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, we will shred paper-based records, and overwrite or delete electronic files.We have large secure bins to collect paper-based records for secure disposal by a third party on the School's behalf. We require the third party to provide sufficient guarantees that it complies with data protection law.

Personal Data Breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The DFO will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their training.

The School will make all reasonable endeavours to minimise the risk of personal data breaches. Where the school faces a data security incident, the DFO will coordinate an effort to establish whether a personal data breach has occurred, assess the significance of any breach, and take prompt and appropriate steps to address it. We will follow the procedure set out in Annex 1. When appropriate, we will report the data breach to the ICO within 72 hours.

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.

Monitoring Arrangements

This policy will be reviewed and updated every 2 years or sooner if legislation or guidance changes.

Links with other policies

This data protection policy is linked to our:

- Admissions Policy Anti-Bullying Policy
- Safeguarding & Child Protection Policy
- Data Protection – Good Practice Guide Equal Opportunities Policy First Aid Policy
- Health & Safety Policy
- Acceptable Use Policy – Staff
- SEND Policy

Annex 1: Personal 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 DFO
- The DFO will investigate the report and determine whether a breach has occurred. To decide, the DFO 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 DFO will alert the Head and the Chair of Governors and will make all reasonable efforts to contain and minimise the impact of the breach,assisted by relevant staff members or data processors where necessary.

The DFO will assess the potential consequences, based on how serious they are perceived to be, and how likely they are to happen

The DFO will make recommendations to the Head and, if required, the Chair of Governors, as to whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DFO 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
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it is likely that there will be a risk to people's rights and freedoms, the DFO must notify the ICO.

- The DFO will document the Governors' decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions will continue to be stored on the Data Controller Log.

- Where the ICO must be notified, the DFO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DFO 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 DFO
- 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 breachand mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DFO 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 DFO expects to have further information. The DFO will submit the remaining information as soon as possible.

The Bursar 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 DFO 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 DFO
- 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 DFO 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 DFO 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 Data Controller Log held on SharePoint.
- The DFO and Head will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to Minimise the Impact of Data Breaches

We will take all the necessary and practicable actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.