NORWICH SCHOOL

Data Protection Policy

This policy is reviewed by the Assistant Bursar annually. This policy was last reviewed and agreed Michaelmas 2025 It is due for review in Michaelmas 2026.

Confirmed by:

Colin Evans	Bursar	Michaelmas 2025

Version Control

The version control table should be updated each time:

- a **change** is made to an **agreed version** of a document; or
- a previously agreed document version is **reviewed with no changes** (i.e. at annual review no changes are required and the document continues to be live for the following year).

Use the following convention: version 1.0 (first version), version 2.0 (major change to version 1.0 and issued as a new version), version 2.1 (second version with minor change)

Version number	Date issued	Author / key contact	Change(s) summary • Minor changes can be authorised by a senior staff member and do not need formal approval. • Major revisions require approval through the confirming authority (typically a Committee)
1.0	Trinity 2022	Khloe Quinn	
	Trinity 2023		No changes
1.1	Michaelmas 2024	Nicole Reynolds	Updated 'AUA' to 'RUA'

Contents page

Purpose and Context

The School is committed to a policy of protecting individuals' right to privacy in accordance with the Data Protection Act 2018 (DPA), [including any replacement of that Act] incorporating the General Data Protection Regulation (GDPR). This policy sets out that commitment. The School recognises that correct and lawful treatment of personal data contributes to the good reputation of the School by demonstrating its integrity and its respect for those it deals with. The School needs to process certain information about its staff, pupils and other individuals it has dealings with. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

Scope

This policy encompasses all processing of personal data by staff, pupils and volunteers, each of whom are subject to this policy. As a matter of good practice, other organisations or agents who have access to and process personal data on behalf of the School, will be expected to have read and comply with this policy. It is the responsibility of the relevant department who deal with such external third parties to ensure that such third parties agree in writing to abide by this policy, with support from published procedures and guidance, and from the School.

This policy also applies to staff and pupils who process personal data off-site. Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and pupils should take particular care when processing personal data at home or in other locations outside the School site and should comply with the School's Responsible Use Agreements and IT Security Policy and Procedures.

Policy Statement

This policy does not form part of the formal contract of employment for staff, but it is a condition of employment that employees will familiarise themselves with and act in accordance with this policy. The School may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be managed in accordance with the School's policy framework.

Any failure to follow this policy by staff or pupils may result in disciplinary action. Any failure by volunteers to follow this policy may result in their access to School IT systems and premises being restricted or removed.

Background

The purpose of the DPA is to protect the rights and privacy of living individuals and to ensure that personal data is processed fairly and transparently.

The School collects, holds and uses personal data relating to individuals who have / have had a relationship with the School.

The purpose of this policy is to ensure that the School:

- Operates procedures and practices that conform to the requirements of the DPA when working with personal data
- Clearly defines responsibilities and accountability for data protection

Provides staff, researchers and pupils with the resources, knowledge, competencies and procedures to work with personal data in compliance with the DPA and with this policy

Breach of the DPA can lead to enforcement action by the Information Commissioner's Office (ICO), which can now impose monetary penalties on the School of up to £17,500,000. The School might also be sued by any individuals affected by the breach. In addition, individuals may also be subject to fines and criminal liability where they are found to have breached the DPA.

Data Protection Definitions

This policy tries as far as possible to avoid using technical terms. However, there are some terms used in the DPA that it is helpful to have an understanding of in the context of data protection compliance. To assist such understanding, we have set out a list of key terms and their meanings below. Where these terms are used in this policy, they should be read and applied in this context.

Data Subject - Any living individual who is the subject of personal data held by an organisation.

Data Controller - In the context of the majority of personal data held by the School, the School will be the Data Controller. A Data Controller is any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data is processed and the way in which the personal data is processed.

Personal Data - Data relating to a living individual who can be identified from that information or from that data combined with other information in possession of the School. Includes name, address, telephone number, student or staff ID number, details of schools attended and photographs (which may also constitute Sensitive personal data). Also includes expression of opinion about the individual, and of the intentions of the School in respect of that individual.

Process or Processing - Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Sensitive personal data / Special Categories of personal data - Means personal data about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic data, biometric data for the purpose of uniquely identifying a person (e.g., fingerprints), data concerning physical or mental health or condition (e.g., substance abuse testing), sexual life, criminal offences, or related proceedings. Any use of Sensitive personal data or Special Category Data must be strictly controlled in accordance with this policy.

Third Party - Any individual / organisation other than the Data Subject or the Data Controller (i.e. the School) or an employee of the School who is processing personal data on behalf of the School in accordance with this policy.

Responsibilities Under the Data Protection Act

The School is the Data Controller in respect of personal data processed by and for the School.

The Assistant Bursar has been appointed as the Data Protection Co-ordinator for the School. In the Assistant Bursar's absence, the Head of Operations will cover as required.

Heads of Department within the School have overall responsibility for the processing of personal data within their own departments and for ensuring that such processing is undertaken in a way that is compliant with this policy. All those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within the School, but ultimately, compliance with data protection legislation is the responsibility of all members of the School who process personal data.

All staff are responsible for:

- Ensuring that they have undertaken School provided data protection training;
- Checking that any information that they provide the School in connection with their employment is accurate and up to date and for informing the School of any changes to their personal data (e.g. change of address); and
- Ensuring that any personal data processed by them is processed in accordance with the DPA and with this policy.

Staff who have a responsibility for supervising / mentoring pupils who are undertaking processing of personal data (e.g., as part of a research project or on a placement) have a responsibility to ensure that the student is informed as to their responsibilities under the DPA, by reference to this policy and other relevant materials.

All pupils / parents and carers are responsible for checking that any information that they provide the School in connection with their enrolment and study at the School is accurate and up to date and for informing the School of any changes to their personal data (e.g. change of address).

Pupils who are considering processing personal data as part of their studies must notify and seek approval from their tutor / head of department. Such pupils will be bound by the DPA and by this policy and must ensure that they act in accordance with both.

Data Protection Principles

The School's policy is to process personal data in accordance with the DPA and rights of individuals as set out below. All staff have personal responsibility for the practical application of the School's data protection policy.

The School will observe the principles set out in the DPA in respect of the processing of personal data and will adhere to the following principles:

- To process lawfully, fairly and transparently.
  Those responsible for processing personal data must make reasonable efforts to ensure that Data Subjects are informed of the identity of the Data Controller (i.e. the School), the purpose(s) and legal basis of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the personal data will be kept.

- To obtain personal data for specific, explicit and legitimate purposes.
  Personal data will not be processed in a manner incompatible with those purposes, and personal data obtained for specified purposes must not be used for a different purpose.

- To ensure that the personal data is adequate, relevant and not excessive in relation to the purposes for which it is used. Information that is not strictly necessary for the purpose for which it is obtained should not be collected. If personal data is given or obtained which is excessive for the purpose, it should be immediately deleted or destroyed.

- To keep personal data accurate and up to date (and where inaccurate ensure they are erased and rectified without delay). Personal data that is kept for a long time must be reviewed and updated as necessary. No personal data should be kept unless it is reasonable to assume that it is accurate.

  It is the responsibility of all individual staff, pupils and other persons to ensure that personal data held by the School is accurate and up to date. Completion by a Data Subject of an appropriate registration or application form, etc. will be taken as an indication that the data contained therein is accurate. Individuals should notify the School of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the School to ensure that any notification regarding change of circumstances is noted and acted upon.

- Not to keep personal data for longer than is necessary for the purposes for which it is used.

- To keep personal data secure to prevent unauthorised or unlawful processing and accidental loss, damage or destruction, using appropriate technical or organisation measures.

- To process personal data in accordance with the rights of data subjects in accordance with the DPA.

- Not to transfer personal data to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The School should generally not process personal data unless:

- It is to fulfil a contract with the individual (be this a parent/carer, a member of staff or a third party)

- The processing is necessary to comply with the School's legal obligations or exercise legal rights

- The processing is required for a task in the public interest, or in the exercise of the School's official authority

- The processing is in the School's legitimate interests and does not unduly prejudice the individual's privacy

To the extent the School processes Special Categories of personal data, it must ensure that such processing satisfies the conditions for processing required by the DPA.

Transparency is key to data protection. Individuals should be told how, why and on what basis their personal data is being processed.

The School will publish privacy notices in respect of its processing of personal data of pupils, staff, alumni, certain partners and visitors, which tell those people:

- what data is collected about them
- what it is used for
- the legal basis for processing the data
- who it will be shared with
- how long it will be held for

When gathering personal data or establishing new Data Protection Activities, members of staff should check existing privacy notices to see whether they need to be updated to reflect the new activities, or whether new privacy notices are required to cover that activity.

There are limited exceptions to the requirement to give Data Subjects notice of processing activities. In any case of uncertainty as to whether a notification should

be given or updated, staff should contact the Assistant Bursar. In the event that staff or pupils process personal data on behalf of another party (as a part of research activities or otherwise), due diligence should be carried out (and contractual protection obtained) to ensure appropriate data protection notices or consents have been given or obtained.

Data Subject Rights

Under the DPA, Data Subjects have the following rights regarding the processing of their personal data and the data that is recorded about them:

- To access personal data held by the School about them
- To require the School to rectify any inaccurate personal data held by it about them
- To require the School to erase personal data held by it about them

This right of erasure will only apply where, for example:

  - The School no longer needs to use the personal data to achieve the purpose it collected it for
  - Where the Data Subject withdraws their consent if the School is using their personal data based on Data Subject consent
  - Where the Data Subject objects to the way the School processes their data and this is upheld

- To restrict the School's processing of the personal data it holds about them. This right will only apply where, for example:

  - The Data Subject disputes the accuracy of the personal data the School holds
  - Where they would have the right to require the School to erase the personal data but would prefer that its processing is restricted instead
  - Where the School no longer needs to use the personal data to achieve the purpose for which it was collected, but it requires the data for the purposes of dealing with legal claims

  In cases where the School has disclosed data to another party, and it is not disproportionate for the School to do so, it will let the recipients of the data know that the School has rectified, erased or restricted its processing of it.

- To receive personal data, which they have provided to the School, in a structured, commonly used and machine readable format (where processing is automated and is either based on consent or is necessary for the

performance of a contract). Data Subjects also have the right to transfer (or require the School to transfer) this personal data to another organisation (for example, a new employer or higher education institution).

- To object to the School's processing of personal data it holds about them (where its justification for processing the data is either that the processing is necessary for the performance of a task in the public interest, or for the purposes of its own legitimate interests).

- To require a review. Data Subjects may ask the School to review any decisions that it has made about them using automated processing.

- To withdraw their consent, where the School is relying on it to process their personal data.

- To prevent processing for the purposes of direct marketing.

The School will have procedures in place to ensure that these rights can be exercised and will publicise these on its website.

If staff or pupils have concerns about the way in which their personal data is being used or processed by the School, they may contact the Assistant Bursar, in the first instance. If after this, they are not satisfied by the School's response they have the right to lodge a formal complaint with the ICO.

Special Categories of personal data

Special Categories of personal data are afforded a higher level of protection by law. It will normally be necessary to have an individual's explicit consent to process Special Categories of personal data, unless exceptional circumstances apply, or the processing is necessary to comply with a legal requirement, including to fulfil its employment duties as an employer.

The consent should be:

- Freely given (i.e. it should not be conditional)
- Specific (i.e. it should set out exactly what is being consented to)
- Informed, (i.e. it needs to identify the relevant data, why it is being processed and to whom it will be disclosed)
- An unambiguous indication of the individual's wishes by which they, by a statement or by a clear affirmative action (i.e. the ticking of an unticked box) signify their agreement

Staff should contact the Assistant Bursar for more information about the conditions to be satisfied to enable processing of Special Category personal data.

The School will not rely on consent for the purposes of processing staff personal data, save in limited circumstances where it can be demonstrated that there is a genuine choice and the consent was freely given. If any member of the School

wishes to process any personal data by relying on consent as a means to do so they must consult the Assistant Bursar for further guidance.

Security of Data

All staff are responsible for ensuring that any personal data (on others) which they hold are kept securely in line with the School's IT Security Policy and Procedure and in appropriate systems and that such data is not disclosed to any unauthorised third party.

All personal data should be accessible only to those who need to use it. A judgment should be made based upon the sensitivity and value of the information in question, but consideration should always be given to keeping personal data:

- in a lockable room with controlled access
- in a locked drawer or filing cabinet
- if computerised, password protected

Personal data must not be stored on removable media (such as USB storage devices, removable hard drives, CDs or DVDs) or mobile devices (laptops, tablets or smart phones) unless it is encrypted or password protected, and the key kept securely. A backup copy should also be kept on the secure school servers. Personal data must not be stored in generic personal cloud services such as Dropbox.

Care should be taken when sending emails that contain personal data.

If personal data is transferred using removable media, a secure, tracked service must be used to ensure safe delivery.

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised individuals.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be securely wiped clean before disposal. If in doubt as to what the correct security measures are for the deletion or disposal of electronic personal data, advice should be taken from IT Support.

Where the School uses external organisations to process personal data on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal data. There are also mandatory legal protections which must be included in any contract with such parties. Any data processing agreement the School enters into must contain such protections.

In the event that the School acts as a Data processor, processing personal data on behalf of a third party, such third party may require additional security arrangements to be implemented. There are also mandatory legal protections which must be included in any contract, which needs to be flowed-down to any sub-processor used by the School.

Members of the School should consult the Assistant Bursar to discuss the necessary steps to ensure compliance when setting up any new agreement or altering any existing agreement.

Reporting Breaches

Members of the School have an obligation to report actual or potential data protection compliance failures to the Assistant Bursar immediately they become aware of them, following the published breach notification procedure. The DPA provide that breaches must be notified to the ICO as soon as possible and in any event within 72 hours of becoming aware of them.

Notification to the Assistant Bursar also allows the School to:

- investigate the failure and take remedial steps if necessary; and
- make any other applicable notifications, including to affected Data Subjects where appropriate.

School staff may be required as part of their duties to support the School in any such investigation.

Where the School is acting as a Data processor, it will have a responsibility to notify actual or potential data protection compliance failures to the third party it is processing personal data on behalf of. The contract between the School and the third party it is processing personal data on behalf of may also have additional contractual restrictions or timescales in respect of such support / assistance. Members of the School should check the contractual position carefully.

Acting as a Data Processor

When the School processes the personal data of pupils, staff, suppliers, alumni, and other individuals (in a professional or personal context) it is ordinarily the case that the School would be known as a Data Controller. A Data Controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

In some limited circumstances, the School may be a Data processor; i.e. it is processing the data on behalf of a third party Data Controller.

If Members of the School are handling personal data and are not sure whether the School is acting as a Data Controller or a Data processor, they should contact the Assistant Bursar in the first instance. It is key to understand the relationship, in order to determine how such personal information should be handled.

The Data Controller has the majority of the obligations under the DPA, (e.g. in respect of Data Subject rights and ensuring appropriate consents are obtained or privacy notices are given.) However, a Data processor also has a number of obligations under the DPA. In most cases, the processing obligations imposed on the School will be guided by the contract entered into between the School and the third party on whose behalf it is processing.

Accuracy, Adequacy, Relevance and Proportionality

Members of the School should make sure data processed by them is accurate, adequate, relevant and proportionate for the purpose for which it was obtained. Personal data obtained for one purpose should generally not be used for unconnected purposes, unless the individual has agreed to this or would otherwise reasonably expect the data to be used in this way.

Individuals may ask the School to correct personal data relating to them which they consider to be inaccurate. If a member of staff receives such a request and does not agree that the personal data held is inaccurate, they should nevertheless record the fact that it is disputed and inform the Assistant Bursar.

Staff and pupils must ensure that personal data held by the School relating to them is accurate and updated as required.

Rights of Access to personal data

Individuals have the right (subject to certain exceptions) to request access in relation to any information held by the School about them in electronic format and / or in manual records which form part of a relevant filing system, save where exemptions apply. A request of this nature is known as a “subject access request”. The request can be made to any member of staff either verbally or in writing (including all electronic methods). All such requests should be referred immediately to the Assistant Bursar. This is particularly important because the School must respond within one month of the initial request being made. In order to assist the School in complying with such requests, it is helpful if the form provided through the School's Data Protection webpages is completed. For information on responding to subject access requests in accordance with the DPA see the guidance available on the School’s website.

Where a request is made for examination scripts (where these are still held), no copies of the scripts will be provided but pupils may view the script in the presence of a representative from the School. Examiners' comments can be transcribed and provided as part of a subject access request.

In order to respond efficiently to data subject rights requests the School needs to have in place appropriate records management practices.

In addition to the above, where the School is acting as a Data processor, it will have a responsibility to provide assistance to the third party it is processing personal data on behalf of, in respect of individuals exercising their rights. The contract between the School and the third party it is processing personal data on behalf of,

may also have additional contractual restrictions or timescales in respect of such support / assistance. You should check the contractual position carefully prior to:

(a) responding to a request made directly by an individual or third party

(b) providing assistance to the third party;

and check with the Assistant Bursar if you are unclear how to proceed.

Disclosure of personal data

The School must ensure that personal data is not disclosed to unauthorised third parties. This includes family members, friends, government bodies, the media, and in certain circumstances, the Police.

All staff and pupils should exercise caution when asked to disclose personal data held by the School about another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's personal details to someone who wished to contact them regarding a non-work related matter, especially when such details are not otherwise publicly available (such as work contact details on the School website). The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of School business.

This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

- where the disclosure is in the legitimate interests of the School (e.g. disclosure to staff – personal data can be disclosed to other School employees if it is clear that those members of staff require the information to enable them to perform their jobs)
- where the School is legally obliged to disclose the data (e.g. minority and disability monitoring, all of which are covered in the School's privacy notices for staff and pupils)
- where disclosure of data is required for the performance of a contract

If personal data is to be shared with a third party in connection with the performance of a contract, then approved data protection clauses must be included in the relevant contract. The School's Assistant Bursar should be consulted on every occasion before any such contracts are entered into and personal data must not be shared with the third party until an appropriate contract is in place.

The DPA permits certain disclosures without notification to the Data Subject in certain cases, so long as the information is requested for one or more of the following purposes:

- to safeguard national security**

- prevention or detection of crime including the apprehension or prosecution of offenders**
- assessment or collection of tax duty**
- discharge of regulatory functions (includes health, safety and welfare of persons at work)**
- to prevent serious harm to a third party
- to protect the vital interests of the individual; this refers to life and death situations.

**Requests must be supported by appropriate paperwork and should follow the agreed protocols if in place. Where a third-party request is received citing one of these grounds, the request should be passed to an authorised person within the School for approval before any information is related.

When members of staff receive enquiries as to whether a named individual is a member of the School (staff or student), the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member of the School may constitute an unauthorised disclosure of personal data.

Unless the Data Subject has requested otherwise, personal data should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the Data Subject consenting to disclosure to the third party should accompany the request.

As an alternative to disclosing personal data, the School may offer to do one of the following:

- pass a message to the Data Subject asking them to contact the enquirer
- accept a sealed envelope / incoming email message and attempt to forward it to the Data Subject
- Please remember to inform the enquirer that such action will be taken conditionally
  (i.e. "if the person is a member of the School" to avoid confirming their membership of, their presence in or their absence from the institution)
- If in doubt, staff should seek advice from the School Assistant Bursar

Retention and Disposal of Data

The School discourages the retention of personal data for longer than it is required. Considerable amounts of data are collected about staff, pupils, applicants etc. However, once a member of staff or a pupil has left the School, or the purpose for which that data was collected has ended, it will not be necessary to retain all the information held on them. Some personal data will be kept for longer periods than others. The School's Retention and Disposal Schedule should be followed for the retention and disposal of personal data.

The School aims to reduce the duplication of personal data and will encourage as far as possible the use of definitive central sources of information for data used across the School (e.g. contact addresses). Those with legitimate reason will have access to the personal data relevant for their job. Permissions granted for such access will be logged where possible and regularly reviewed.

The creation of systems and / or files which duplicate such data should be avoided; where it is inevitable every care should be taken to ensure that data maintained in subsidiary systems is fully synchronised with definitive sources, and updated frequently through secure and reliable interconnection.

Pupils

In general, electronic student records maintained in the School's MIS are kept permanently in order to fulfil the requirement for the provision of transcripts during a pupil's or former pupil's working life. Such information would typically include name and address on entry and completion, subjects taken, examination results and awards obtained.

The School should regularly review the personal files that they hold relating to individual pupils (whether stored electronically or in paper records) in accordance with the School's Retention and Disposal Schedule.

Staff

In general, electronic staff records containing information about individual members of staff are kept indefinitely and information would typically include name and address, positions held, leaving salary. Other information relating to individual members of staff will be kept by Human Resources for six years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay, etc. will be retained for the statutory time period (between three and six years).

Staff records are kept and maintained by Human Resources. Other departments should only keep staff information where necessary for legitimate business purposes. To the extent that files of individual staff members are kept outside Human Resources, departments should regularly review those files of in accordance with the School's Retention and Disposal Schedule.

Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for six months from the interview date and should then be securely destroyed as confidential waste. Human Resources may keep a record of names of individuals that have applied, been short-listed, or interviewed, for posts indefinitely. This is to aid management of the recruitment process.

Disposal of Records

Personal data must be disposed of in a way that protects the rights and privacy of Data Subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion) and in line with the School's Retention and Disposal Schedule.

International Transfers

Data must not be transferred outside of the European Economic Area (EEA) - the twenty-eight EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual, or unless the personal data is adequately protected or an exemption applies.

Adequate protection can be provided if:

- The data protection arrangements in the destination country have been approved by the ICO (there is a list of approved countries on the ICO website); or
- The recipient is a signatory to an ICO approved data protection regime; or
- The recipient is bound by a contract that ensures that the personal data concerned will be adequately protected (for example, incorporating the Standard Contractual Clauses approved by the ICO).

Members of the School should be particularly aware of this when contracting with a third party for the processing of personal data (including for IT support, collaborative provision, or research purposes) or when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a website that can be accessed from outside the EEA.

In addition to the above, where the School is acting as a Data processor, the contract between it and the third party it is processing personal data on behalf of may have additional contractual restrictions in respect of international transfers of such data. Members of the School should check the contractual position carefully prior to transferring the personal data and check with the Assistant Bursar if they are unclear how to proceed.

Publication of School Information

The School publishes a number of items that include personal data, and will continue to do so. These include:

- Names of all members of School Committees
- Staff Telephone and Email Directory
- Information in prospectuses (including photographs), annual reports, staff newsletters, etc.
- 'Graduation' programmes and videos or other multimedia versions of graduation ceremonies
- Publicity information included in public relations stories and press releases and on social media
- Staff information on the School website (including photographs).

It is recognised that there might be occasions when a member of staff, a pupil, or other party, requests that their personal details in some of these categories remain

confidential or are restricted to internal access. All individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, the School should use its reasonable endeavours to comply with the request and ensure that appropriate action is taken.

Direct Marketing

Any proposal to carry out direct marketing (i.e., marketing by email, telephone, post or any other means that is directed at a particular individual, whether they are a pupil, applicant, alumnus, member of staff or otherwise) must be reviewed and approved in advance by the School Assistant Bursar in conjunction with the Marketing team.

Members of the School should not send direct marketing material to someone electronically (e.g., by email, Whatsapp, social media messenger services or targeted banner ads) unless there is an existing business relationship with them in relation to the services being marketed. Staff should abide by any request from an individual not to use their personal data for direct marketing purposes and should notify the relevant marketing team about any such request.

Any department that uses personal data for direct marketing purposes must inform Data Subjects of this at the time of collection of the relevant personal data and may only make direct marketing communications where the Data Subject has opted-in to receiving such communications. Data Subjects must also be given the opportunity to opt out of receiving communications at any time, and measures must be put in place to prevent such communications from being sent once the School has received confirmation that a Data Subject has opted out.

Use of CCTV

The School's use of CCTV is regulated by a separate Code of Practice.

For reasons of personal security and to protect School premises and the property of staff and pupils, close circuit television cameras are in operation in certain site locations. This policy determines that personal data obtained during monitoring will be processed as follows:

- Any monitoring will be carried out only by a limited number of specified staff
- The recordings will be accessed only by those specified staff
- Personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete in line with the School's Retention and Disposal Schedule
- Staff involved in monitoring will maintain confidentiality in respect of personal data

Academic Research

Personal data collected only for the purposes of academic research (including work of staff and pupils) must be processed in compliance with the DPA. The School will publish additional guidance to assist researchers in complying with these requirements.

Individual pupils or staff carrying out research should note that personal data may be processed for research purposes on the legal basis that the processing is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the School. Researchers may also rely on the bases that the processing is necessary for scientific or historical research purposes, or that it is necessary for statistical purposes.

Where the legal bases for processing personal data referred to above are available to researchers, the consent of the Data Subject is not required. However, such processing is subject to safeguards to ensure that data is minimised (including being pseudonymised, and if possible anonymised) and that:

- The personal data is not processed to support measures or decisions with respect to particular individuals
- The Data Subjects must not be caused substantial damage or substantial distress by the processing of the personal data

If the above conditions are met, together with technical and organisational safeguards to keep data secure, personal data processed for research purposes may be:

- Processed for purposes other than that for which it was originally obtained, including statistical or historical purposes
- Exempt from the Data Subject's right of access and rectification, as well as their right to restrict or object to processing

Other than this, the DPA applies in full in respect of academic research. The obligations to collect only necessary and accurate personal data, to hold personal data securely and confidentially and not to disclose personal data except in accordance with the DPA (including in relation to publication) must all still be complied with.

Publication

Researchers should ensure that the results of research are anonymised when published and that:

- No information is published that would allow individuals to be identified (including where anonymised data could be matched with other data to link back to an identifiable individual)
- Where consent has not been obtained for such use from the Data Subject
- Where the nature of the research makes it impracticable or otherwise undesirable to attempt to seek / obtain consent, that there is a legitimate

interest in publication and publication would not unfairly damage the rights and freedoms of the Data Subject

Data Protection Impact Assessment (PIA)

The School encourages all staff to incorporate 'Privacy by Design' into their activities which involve processing personal data - an approach by which data protection is built into a project from the outset and not bolted on at the end. The Privacy Impact Assessment (PIA) is a method by which the School can assess and address the risk of processing and identify measures to support Data Protection.

The PIA involves setting out the envisaged processing, its purposes, and the legal basis under which it is to be processed. It involves an assessment of the risks posed by the processing to the rights and freedoms of the Data Subjects, and the measures to be taken to address those risks. It will include an analysis of safeguards being put in place and will demonstrate how the processing will be compliant with the DPA. Once the School has carried out a PIA, it will keep it under regular review to ensure that the assessment of risk addresses circumstances as they change.

To help the School meet its data protection obligations and to meet staff and pupils' expectations of privacy, the School carries out PIAs prior to beginning any new processing activities.

These are only required under the DPA for:

- The large-scale processing of sensitive personal data
- Systematic monitoring of a public area on a large scale
- The systematic evaluation of individuals based on automated processing
- Other processing activities which are likely to result in a high risk to the rights of Data Subjects

It is good practice to carry out PIAs when embarking on new projects involving the processing of personal data and staff are encouraged to do so, however where this is not the case, staff are still encouraged to consider Data Protection compliance when starting any new processing activity, to ensure it is conducted in line with this policy.

The data protection regulator in the UK also requires PIAs to be carried out where an organisation plans a number of specific processing activities, including using new technology, processing biometric data or collecting personal data from a source other than the Data Subject without providing them with a privacy notice.

Document control

Document title:	Data Protection Policy
Prepared by:	Nicole Reynolds, Assistant Bursar
Authorised by:	Colin Evans, Bursar
Published location(s):	▪ Norwich School Website ▪ Norwich School Hub
Other internal policies / documents referenced:	▪ Responsible Use Agreement
External documents referenced:	▪ DPA 1998 (DPA) ▪ General Data Protection Regulation (GDPR)