KINGS NORTON GIRLS' SCHOOL

Selly Oak Road · Birmingham · B30 1HW

Telephone: 0121 675 1305

Website: www.kngs.co.uk · Email: enquiry@kngs.co.uk

DATA MANAGEMENT including:

GENERAL DATA PROTECTION REGULATION (GDPR) AND RETENTION OF RECORDS POLICY AND GUIDANCE

Reviewed: March 2024
Review Date: March 2027
Review Cycle: 3 years
Author: CSK
Committee: Resources

1. Aims

Our school aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. Thus, demonstrating our core values of respect and courage in order to flourish.

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 expected 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. Definitions

Term	Definition
Data	Information in whatever form (including, without limitation, in written, oral, visual or electronic form or on any magnetic or optical disk or memory and wherever located) relating to the business, products, affairs and finances of the school for the time being confidential to the school and trade secrets including, without limitation,

	technical data and know-how relating to the business of the school or any of its suppliers, clients, customers, agents, distributors, shareholders or management, including personal data.
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our school processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

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

5. Roles and responsibilities

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

5.1 Governing board

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

To support this, the Governing Body has appointed a link governor for GDPR who can be contacted via the Clerk to the Governing Body.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

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

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

Our DPO is Clare Skinner and is contactable via hrdp@kngs.co.uk inserting FAO DPO in the subject line or on 0121 675 1305. Clare Skinner can also be written to at Kings Norton Girls' School, Selly Oak Road, Birmingham B30 1HW.

5.3 Headteacher

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

5.4 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 DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes

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

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

7. Privacy Information

The school's obligations under the GDPR include providing specific information to data subjects on the information that the school collects, retains and generally processes. This requirement is to be transparent in the way that the school processes personal data.

Transparency means that KNGS is required to specify the purposes for which the school processes personal data, how long the school may hold the information for and what the data subject's rights are.

Details of this are included within the school's privacy information. All employees must be familiar with the privacy information because it contains details about how the school, and therefore how employees, may process personal data and the reasons why.

Crucially, KNGS is not allowed to process personal data for a purpose that is incompatible with one of the stated purposes in the school's privacy information. While the school has sought to identify all the purposes for which KNGS processes personal data in the school's privacy information, it may be that the stated purposes have to be extended in certain circumstances. Any issues that arise in relation to this should be referred to the DPO.

If staff are unclear about their obligations and duties or require assistance with any of the privacy information they must speak to the DPO for guidance.

Students deemed to be of a suitable age (usually 13+) are also made aware of the privacy information, the school's legal obligations to pass on certain information, e.g. to providers of youth support services, and their rights to request the school to withhold certain information.

KNGS privacy information for parents, guardians and pupils are worded incorporating the current DFE template and its circulation is supervised by our DPO. They are available on the school website.

8. Collecting personal data

8.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) 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 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/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 sell 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.

8.2 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 the school's record retention schedule/records management policy.

9. Sharing personal data

We will not normally share personal data with anyone else, but may do so 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 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 students or staff.

We might need to share pupils' information with placement students, completing work experience as part of their university degree. Access will only be granted if it is relevant to their work. For more information, please see the KNGS 'Student Placement Policy'.

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. This potentially applies to foreign trip organisation and online surveys. Staff understand that they should check with the DPO prior to sending personal data outside of the EEA.

10. Subject access requests and other rights of individuals

10.1 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

Individuals can make Subject Access Requests in any format. This includes verbal requests, or written requests via letter, text or email. Once an individual has made a request, they cannot be asked to change the format they made the request in.

If staff receive a subject access request they must immediately forward it to the DPO.

10.2 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 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, most subject access requests from parents or carers of students at our school may not be granted without the express permission of the student. Individual student's ability to understand their rights will always be judged on a case-by-case basis.

10.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual for clarification of what specific information they are looking for
- Will make reasonable efforts to search through all records
- 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 30 days 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 multiple. We will inform the individual of this within 30 days, and explain why the extension is necessary

If the deadline for a response falls on a weekend or bank holiday, we may respond on the next working day.

We will not disclose information if it:

- Might cause 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
- Being used by a court in proceedings concerning the child

If the requester already has access to the information they wish to see, they may be directed to this. For example, the requester may already have access to personal data stored on the school's website. This request does not have to be treated as a SAR, provided they can access the information within one calendar month.

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.

Where a request is deemed to be unfounded or repetitive, the data subject will be informed of the reason and given an opportunity to appeal.

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

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

- Withdraw their consent to processing at any time
- 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 e.g. foreign trips
- 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 DPO.

11. Parental requests to see the educational record

Parents, or those with parental responsibility, we will provide appropriate access to their child's educational record (which includes most information about a student) within 30 days of receipt of a written request to the DPO.

12. 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. For example, students can be provided with a PIN in order to pay for school dinners at each transaction if they wish.

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.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

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.

13. 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 Network Manager.

14. Photographs and videos

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

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will 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 magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages
- As part of curriculum assessments which will be provided to exam boards and external moderators

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 only accompany them with any other personal information about the child where consent is provided to do so. See our child protection and safeguarding policy and photography policy for more information on our use of photographs and videos.

15. 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:

- 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 relevant documents
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters
- 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 information)
    - 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

16. 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 and portable electronic devices, such as laptops and hard drives that contain personal data should be kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff are aware of the requirement to keep it secure at all times
- Passwords that meet Microsoft's standard complexity requirements are used to access school computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our ICT acceptable policy)
- 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)

17. 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, we 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.

A retention schedule can be found in Appendix 2.

18. Personal data breaches

The school will make all reasonable endeavours 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, we will report the data breach to the ICO and, in some circumstances, the data subject of any personal data breaches within 72 hours of becoming aware of the breach. 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 student premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about students

We have put in place protocol to deal with any suspected personal data breach and will notify the appropriate personnel where it is necessary to do so.

If you know or suspect that a data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO and retain all evidence of the suspected breach so that the matter can be properly investigated.

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. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

The school has also appointed a link governor for Data Protection who can be contacted via the Clerk to the Governing Body.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any statutory changes are made that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 3 years** and shared with the full governing board.

21. Links with other policies

This data protection policy is linked to our:

Safeguarding and child protection policies
ICT Acceptable Use policies
Freedom of Information publication policy
Student Placement policy

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

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are on the school's computer system.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO

- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

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

  Records of all breaches will be stored on the school's computer system

  The DPO and Headteacher will meet to review what happened and how it can be prevented from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

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

As part of policy review, the school will regularly carry out a risk assessment to establish what security measures are already in place and whether or not they are the most appropriate and cost effective available. The school's data protection officer is also responsible for the completion of the risk assessment.

Carrying out a risk assessment will generally involve answering the following questions:

- How sensitive is the data?
- What is the likelihood of it falling into the wrong hands?
- What would be the impact of the above?

Does anything further need to be done to reduce the likelihood?

When these questions have been answered, the DPO will be able to recognise the risks that are present, judge the level of those risks and prioritise them. Once the risk assessment has been completed, the school can decide how to reduce any risks or whether they are at an acceptable level.

Appendix 3 offers staff guidance for assessing the risk of sharing information.

Risk assessment will be an on-going process and the school will carry out assessments at regular intervals because risks change over time.

Appendix 2: Timescales for Retention of Records

Employment records

1	Payroll records	Previous 6 tax years plus current
2	Tax credits	3 months after relevant tax year
3	Statutory Sick Pay (SSP)	3 years after end of relevant tax year to which they relate
4	Statutory Maternity Pay (SMP)	3 years after end of relevant tax year to which they relate
5	Statutory Adoption Pay (SAP)	3 years after end of relevant tax year to which they relate
6	Statutory Paternity Pay (SPP)	3 years after end of relevant tax year to which they relate
7	Parental Leave	Optional up to 18 years
8	Flexible Working Request	1 year
9	Disciplinary warnings/appeals	Retain on file deleting through warning issued

Other records

- School records for a child should be kept for 7 years after the child leaves the school, or until the child reaches 25 years of age (whichever is greater) and examination records the same.
- Staff personal files should be retained for seven years after the termination of employment and then disposed of securely. Pre-employment vetting information, including DBS checks, should be kept for six months and then disposed of securely.
- Interview records, CVs and application forms for unsuccessful applicants are kept for 6 months.
- All formal complaints made to the Headteacher or School Governors will be kept for at least seven years in confidential files, with any documents on the outcome of such complaints. Individuals concerned in such complaints may have access to such files subject to data protection and to legal professional privilege in the event of a court case.

Appendix 3

Staff help sheet for assessing risk of sharing information

In deciding the most appropriate way to share information and the level of security required, always take into consideration the nature of the information and the urgency of the situation, that is, take a risk-based approach to determining appropriate measures. The simplified process described below will help members of staff and the school itself choose the appropriate level of security needed when sharing potentially sensitive information. The data protection officer is responsible for ensuring that staff are trained to use this process.

Step 1

Imagine a potential security breach (e.g. a confidential letter is left in a public area, a memory stick is lost or someone reads information on a computer screen while waiting to meet a member of staff), and consider:

- Will it affect or identify any member of the school or community?
- Is there a risk of discomfort/slur upon someone's character?
- Is anyone's personal safety at risk?
- Will it embarrass anyone?

If the answer to all the above questions is 'no', the document does not contain sensitive information. If the answer is 'yes' to any of the questions above then the document will include some sensitive information and therefore requires a level of protection.

Step 2

Imagine the same potential security breach as above, and consider:

- Will it affect many members of the school or local community and need extra resources locally to manage it?
- Is someone's personal safety at a moderate risk?
- Will someone lose his or her reputation?
- Will a company or organisation that works with the school to be adversely affected?

If the answer to any of the above questions is 'yes' then the document contains sensitive information and additional security must be considered and the email should be encrypted before you email it to a colleague outside of the school. However, if you think that the potential impact exceeds that stated in the question (e.g. someone's personal safety is at high risk) think very carefully before you release this information at all.

Step 3

All documents that do not fit into steps 1 or 2 might require a higher level of protection/security if released at all. Err on the side of caution and seek guidance from the relevant line manager/senior member of staff.