John Burns Primary School



Data Protection Policy 2026

Reviewed by the Governing Body: Summer 2026

Next Review: Summer 2027

Signed:

Contents

1. Aims 3
2. Legislation and guidance 3
3. Definitions 3
4. The data controller 4
5. Roles and responsibilities 4
6. Data protection principles 5
7. Collecting personal data 6
8. Sharing personal data 6
10. Parental requests to see the educational record 7
11. CCTV 7
12. Photographs and videos 8
13. Data protection by design and default 8
14. Data security and storage of records 9
15. Disposal of records 9
16. Personal data breaches 9
17. Training 9
18. Monitoring arrangements 9
19. Links with other policies 10

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR). and the provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

All staff at John Burns School involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities in:

- Adhering to these guidelines
- Recognising the importance of following the principles of the Data Protection Act 2018; and
- Making sure that information is securely and appropriately managed

2. Legislation and guidance

This policy meets the requirements of the UK GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK 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 regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
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 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, pupils, staff, governors, visitors and others, and therefore is a data controller. The Headteacher is the Senior Information Risk Officer (SIRO).

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 body

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

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 body and, where relevant, report to the governing body 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.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Gary Hipple and is contactable at: schoolsdpo@richmondandwandsworth.gov.uk

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 UK 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. Collecting personal data

7.1 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 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 UK GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (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.

7.2 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.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil 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 pupils – 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 pupils and staff safe while working with us

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

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

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

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.

9. Other data protection rights of the individual

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
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11. 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 Mrs. M. Buckley (School Business Manager).

12. 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 for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

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

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified. If it is necessary to name a pupil alongside a photograph, permission will always be obtained.

See our Child Protection and Safeguarding Policy, Photography Policy and Social Media Policy for more information on our use of photographs and videos.

13. 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 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 a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

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 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 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 for school trips/residentials, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff are forced to change their passwords every 90 days
- All portable devices are protected with login credentials
- Staff, pupils 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 Online safety policy/Computing Policy/Acceptable Use Agreement)

15. 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.

We will shred paper-based records, and overwrite or delete electronic files.

16. 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 our Data Breach Procedure.

When appropriate, we will report the data breach to the DPO within 72 hours.

17. Training

All staff and governors are provided with data protection training as part of their induction process. This will include training completed via an online module.

Data protection will also form part of continuing professional development. This will be carried out by all members of staff and governors at least every two years.

18. Monitoring arrangements

This policy will be reviewed **every 2 years** and shared with the full governing board.

19. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Child Protection and Safeguarding Policy
- Online Safety Policy
- Acceptable Use Agreements
- Photographic Images and Video Policy
- Social Media Policy
- CCTV Policy
- Health & Safety Policy

We supply this information based on your original request. Please do not hesitate to contact me at the above address, should you have any queries regarding the information enclosed.

APPENDIX 1

Subject Access Requests

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

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

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

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

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

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 below the age of 12 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 carers of pupils at our school may be granted without the express permission of 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:

- 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 (term time only)
- 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

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 child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
• Is contained in adoption or parental order records
• Is given to a court in proceedings concerning the child

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

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

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

When to re-submit a request

You can ask the school for access more than once. However, we may be able to refuse access if your request is, as the law says, 'manifestly unfounded or excessive'.

If you are thinking of resubmitting a request, you should think about whether:

• it is likely that your data has changed since your last request
• enough time has passed for it to be reasonable to request an update on how your data is being used, or
• the school has changed its activities or processes recently.

What to do if you disagree with the outcome or remain dissatisfied

If you are unhappy with how the school has handled your request, you should first make a complaint to the school.

Having done so, if you remain dissatisfied you can make a complaint to the ICO at: https://ico.org.uk/concerns/

You can also seek to enforce your rights through the courts. If you decide to do this, we strongly advise that you seek independent legal advice first.

What the school should do

If the school reasonably needs more information to help find your data or identify you, we may have to ask you for the information we need. We may then wait until we have all the necessary information before dealing with your request.

When we respond to your request, the school should provide you with a copy of your data. We may do this electronically. If you need your data in another format, you must ask if this is possible.

You are also entitled to be told the following things:

•What it is using your data for?
•Who is the school sharing your data with?
•How long the school will store your data?
•Information on your rights to challenge the accuracy of your data, to have it deleted, or to object to its use.
•Your right to complain to the ICO.
•Information on where your data came from.
•If the school has transferred your data to a third country or an international organisation, what security measures we took.

When can the school refuse a Subject Access Request

The school may refuse your subject access request if your data includes information about another individual, except where:

•the other individual has agreed to the disclosure, or
•it is reasonable to provide you with this information without the other individual's consent.

In deciding this, the school will have to balance your right to access your data against the other individual's rights regarding their own information.

The school can also refuse your request if it is 'manifestly unfounded or excessive'.

In any case the school will need to tell you and justify its decision. The school should also let you know about your right to complain to the ICO, or through the courts.

How long should the school take to respond?

The school has one month to respond to your request. In certain circumstances it may need extra time to consider your request and can take up to an extra two months. If we are going to do this, we will let you know within one month that we need more time and why.

Can the school charge a fee for this.

A copy of your personal data should be provided free. The school may charge for additional copies. The school can only charge a fee if we think the request is 'manifestly unfounded or excessive'. If so, we may ask for a reasonable fee for administrative costs associated with the request.

APPENDIX 2

Letter template

[Your full address]

[Phone number]

[The date]

[Name and address of the school]

Dear Sir or Madam,

Subject access request

[Your full name and address and any other details to help identify you and the data you want.]

Please supply the data about me that I am entitled to under data protection law relating to: [give specific details of the data you want, for example:

•my personnel file
•emails between 'person A' and 'person B' (from 1 June 2017 to 1 Sept 2017)
•my medical records (between 2014 and 2017) held by 'Dr C' at 'hospital D'
•CCTV camera situated at ('location E') on 23 May 2017 between 11am and 5pm

If you need any more data from me, or a fee, please let me know as soon as possible. It may be helpful for you to know that data protection law requires you to respond to a request for data within one calendar month.

If you do not normally deal with these requests, please pass this letter to your Data Protection Officer, or relevant staff member. If you need advice on dealing with this request, the Information Commissioner's Office can assist you. Its website is ico.org.uk or it can be contacted on 0303 123 1113.

Yours faithfully,

[Signature]

Remember to:

•Keep a copy of your request.
•Keep any proof of postage or delivery.

APPENDIX 3

Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioners Office (ICO).

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Officer (DPO).

Roles and Responsibilities

The Data Protection Officer (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 accidently 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 document.

The DPO will assess the potential consequences based on how serious they are and how likely they are to happen.

The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.eg. emotional stress), including through:

- Loss of control over their data
- Discrimination
- Identity 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 is 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 stored on the schools 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 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 consequence 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. The 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 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:

• 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 schools computer system.

The DPO and Headteacher 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 the actions set out below 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.

Sensitive information being disclosed via email (including safeguarding records)

• If special category data (sensitive information) is accidentally made available via email to unauthorized individuals, the sender must attempt to recall the email as soon as they become aware of the error
• Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
• If the sender is unavailable or cannot recall the email for any reason the DPO will ask the IT department to recall it.
• In any cases where the recall is unsuccessful the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
• The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
• The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

APPENDIX 4

Data Security

Strategic and operational practices

At this school staff are clear who the key contact(s) for key school information are (the Information Asset Owners). We have listed the information and information asset owners in a spreadsheet available on the school database.

We ensure staff know to immediately report, and who to report to, any incidents where data protection may have been compromised, such as when passwords for sensitive systems or devices are lost or stolen, so that relevant action(s) can be taken.

All staff are DBS checked and records are held in one central record in SIMS.

We ensure ALL the following school stakeholders sign an Acceptable Use Agreement. We have a system so we know who has signed:

• Staff

• Governors

• Pupils

• Parents

• Volunteers

This makes clear all responsibilities and expectations with regard to data security.

• We have approved educational web filtering across our wired and wireless networks.

We also have <an additional layer of monitoring software across our network system>.

We monitor school <emails / blogs / online platforms, etc.> to ensure compliance with the Acceptable Use Agreement. As well as monitoring usage, we may also monitor content of e-mails / blogs / etc.

We follow Local Authority guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.

All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private.

We require staff to use STRONG passwords for access into our MIS system.

We require staff to change their passwords into the MIS, USO admin site, every 90 days.

We require that any personal/sensitive material must be encrypted if the material is to be removed from the school, and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without the need to take data home.

School staff who set up usernames and passwords for e-mail, network access, work within the approved system and follow the security processes required by those systems.

We ask staff to undertake house-keeping before they leave the school to review, remove and destroy any digital materials and documents which need no longer be stored. The staff account is deleted when the staff member leaves the schools service.

Technical or manual solutions

Staff have secure area(s) on the network to store sensitive documents or photographs.

We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.

We use RAv3/VPN solution with its 2-factor authentication for remote access into our systems.

We use the DfE S2S site to securely transfer CTF pupil data files to DfE / other schools.

We use the Pan-London Admissions system to transfer admissions data. Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.

We use LGfL AutoUpdate for creation of online user accounts for access to services and online resources.

All staff and governors use LGfL staffmail for all school related email.

We also use LGfL's USO-FX2 to transfer documents to schools in London, such as references, reports of children.

We use LGfL's myDrive for online document storage for our Governing Body.

We store any sensitive/special category written material in lockable storage cabinets in a lockable storage area.

All servers are in lockable locations and managed by DBS-checked staff.

We use LGfL's GridStore remote secure back-up for disaster recovery on our network / admin, curriculum server(s).

We comply with the WEEE directive on equipment disposal, by using an approved disposal company for disposal of IT equipment. For systems, where any protected or restricted data has been held, (such as servers, photocopiers), we get a certificate of secure deletion.

Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.

Paper based sensitive information is shredded, using a cross-cut shredder.