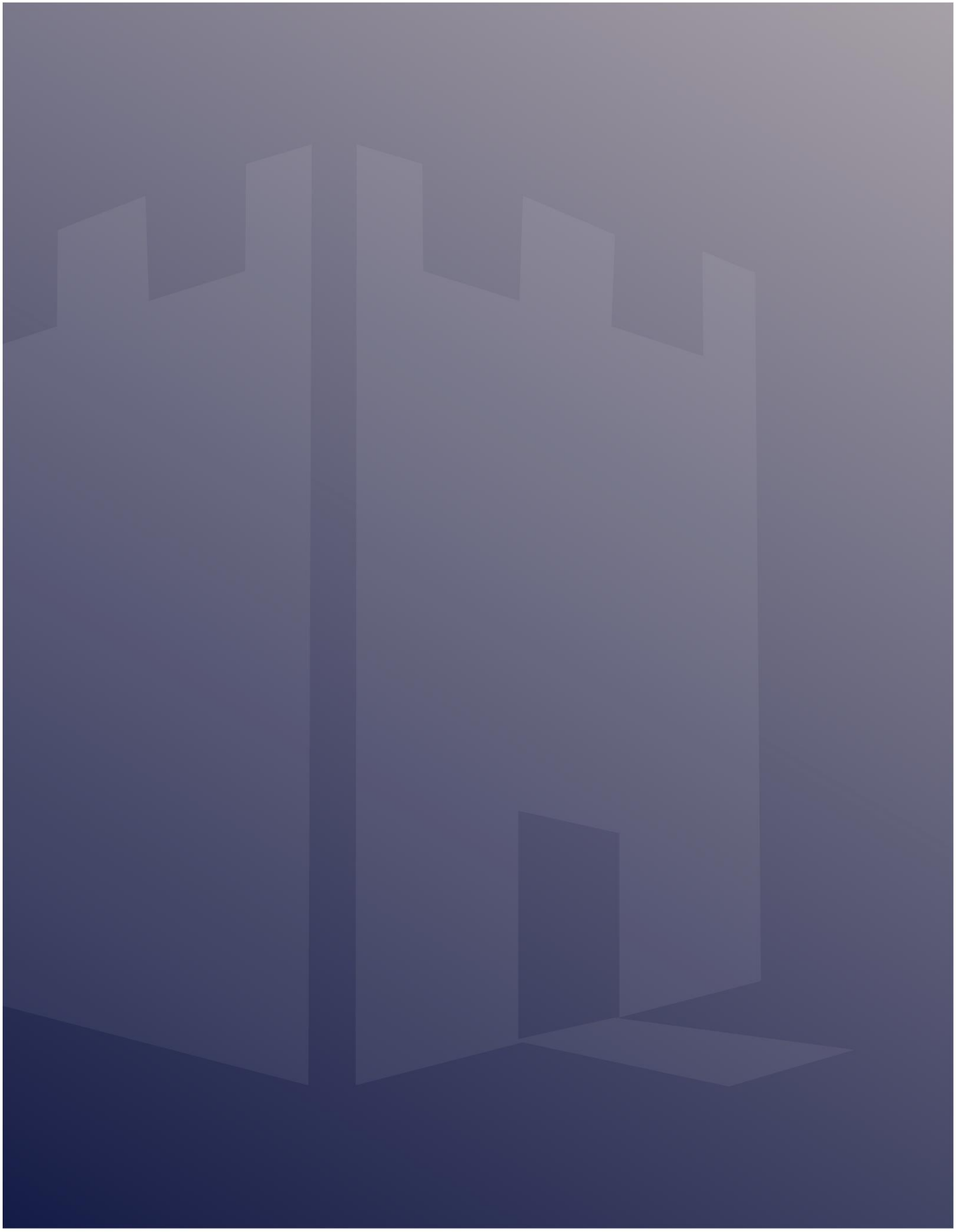
PONTEFRACT
ACADEMIES TRUST

Information Policy



Summary:

This policy is to ensure that the Trust complies with the requirements of the General Data Protection Regulation (UK GDPR), Environmental Information Regulations 2004 (EIR) and Freedom of Information Act (FOIA), associated guidance and codes of practice issued under legislation.

Author	Head of Governance		
Applies to: (please check as appropriate)	Staff ✓	Pupil ✓	Community
Ratifying Committee(s):	Audit and Risk Committee		
Available on:	Compliance Library ✓	Website ✓	
Date of Approval:	12/12/2022		
Date of Next Formal Review: (ensure this is aligned to committee meeting dates)	12/12/2025		
Review Period:	Triennial		
Status:	Non-contractual		
Owner:	**Pontefract Academies Trust**		
Version:	03		

Document Control

Date	Version	Action	Amendments
14th December 2022	01	New Policy	
12th July 2022	Draft 1.1	Remove reference to old IT service provider and any software relating to their service provision	• Whole document updated to reflected introduction of Head of Governance role • Under Disposal of Data section - Airedale Computers replaced by RM Education • Annex 3 – Firewall provision provided by RM Education not Alamo • Security software is now Safetynet not Censurnet •
3rd October 2022	02	Approved to release ARC & Trust Board	
12th December 2022	03	Approved to release ARC & Trust Board	• Removed the reference to requests processed under the Education (Pupil Information) (England) Regulations 2005 as this is not applicable to Academy Trusts • GDPR replaced with UK GDPR • Introduction of Information Security Incident Guidance (Appendix A) • Information Security Incident Reporting and Investigation Form updated in line with DPO audit recommendation (Appendix E)

Contents

1. Purpose, scope, definitions and principle

Purpose

Pontefract Academies Trust ("The Trust") is required to collect, hold, process and share information to enable it to operate. This policy is to ensure that the Trust complies with the requirements of the General Data Protection Regulation (UK GDPR), Environmental Information Regulations 2004 (EIR) and Freedom of Information Act (FOIA), associated guidance and codes of practice issued under legislation.

Where this policy refers to the Trust it will be referring to information held and processed by the following schools in addition to that of the central team:

- Carleton High School
- Carleton Park Junior & Infant School
- De Lacy Primary School
- Halfpenny Lane Junior Infant & Nursery School
- Larks Hill Junior & Infant School
- Orchard Head Junior, Infant & Nursery School
- The King's School
- The Rookeries Carleton Junior, Infant & Nursery School

Scope

The Information Policy covers the following areas and requirements of UK GDPR:

- Data protection.
- Freedom of information.
- Information security.
- Information security incident reporting.
- Records management.
- CCTV surveillance.

The Information Policy applies to information in all forms including, but not limited to:

- Hard copy documents printed or written on paper.
- Information or data stored electronically, including scanned images.
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer.
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card.
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops.
- Speech, voice recordings and verbal communications, including voicemail.
- Published web content for example internet and intranet.
- Photographs and other digital images.

Data controller

The Trust is the Data controller as defined in the Data Protection Act 2018 and is registered with the Information Commissioners Officer (ICO) as registration number **ZA021300**. The details of this registration can be found on the following link to the ICO website:

https://ico.org.uk/ESDWebPages/Entry/ZA021300

The Trust will renew the registration annually in October of each year. If the Trust introduces any new purposes for processing personal information, then it will notify the ICO, requesting that the new purpose be included in the registration.

Data protection officer

The Trust has appointed a Data Protection Officer (DPO) and informed the ICO of this appointment:

Schools Data Protection Officer
Veritau Ltd
County Hall, Racecourse Lane
Northallerton, DL7 8AL
schoolsDPO@veritau.co.uk
01609 532526

The DPO is a statutory position and will operate in an advisory capacity. The duties will include:

- acting as a point of contact for the ICO and data subjects
- facilitating a periodic review of the corporate information asset register and information governance policies.
- assisting with the reporting and investigation of the information security breaches,
- providing advice on all aspects of data protection as required, including information requires, information sharing and data protection impact assessments.
- reporting to the Trustees on the above matters.

Definitions

Personal data is any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person.

In effect, this includes such things as IP addresses, biometric data, as well as genetic data.

The UK GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Sensitive personal data is information that relates to race and ethnicity, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health, sex life, sexual orientation. There are greater legal restrictions on processing sensitive personal data than there are on personal data. It must always be adequately protected.

UK GDPR principles

In accordance with the requirements outlined in the UK GDPR, anyone handling information in the Trust or on behalf of the Trust will have a responsibility to ensure that personal data will be:

- processed lawfully, fairly and in a transparent manner in relation to individuals.

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Related policies or procedures

The information policy will be read in conjunction with the staff code of conduct, including safer working practice guidance.

Complaints

Any complaints about the way which personal data has been handled should contact the DPO on the address set out in paragraph 1 of this policy.

Any complaints in relation to a freedom of information or environmental regulations requests should be made in accordance with the Trust Complaints Policy.

2. Links with other policies or legislation

Head of Governance

The Head of Governance is responsible for ensuring that information risks are assessed and mitigated to an acceptable level. This includes ensuring that all individuals involved in governance, employees and any other authorised trust/school users are aware of their obligations under this policy and related procedures and are given the necessary support and training to meet their obligations.

Headteachers

Each Headteacher is responsible for the management of information risk in their school and for any services/third party processors contracted for directly by the school. This includes:

- ensuring the security and use of information assets.
- annual review of the information asset register and informing the DPO of any significant changes to the information assets as soon as possible.
- ensure that data protection impact assessments undertaken in accordance with this policy.
- ensure that records are maintained and disposed of in accordance with the records management policy.
- ensure that all information security incidents are handled in accordance with the Information Security Incidents Reporting policy.

Information champions

Each school will nominate an information champion who will be responsible for:

- assisting with the development of an information culture within the school.
- communicating key announcements from the DPO/central team within the school.
- identifying where potential information security risks may be apparent.
- having the knowledge and training required to ensure UK GDPR considerations are identified and supported appropriately by the central team and DPO.

Responsibility of all employees

All employees have responsibility for data protection and must read, understand, and adhere to any policies and procedures that relate to personal data that they may handle and undertake any associated training provided.

All employees must understand the main concepts of data protection legislation and report any risks to the security of personal data processed to their line manager immediately.

All employees must be aware of the Freedom of Information Act and what it means.

Training

The Head of Governance will ensure that appropriate guidance and training is given to trustees, SPRB members, employees and other authorised trust/school users. This will include where appropriate access to information procedures, records management, data breach procedures, information security including using email and the internet.

- All staff will be trained every two years in UK GDPR and information security through training approved by the DPO.
- Staff with significant administrative roles will be trained in other aspects of UK GDPR.
- The Trust will ensure that any party contracts / processors have adequately trained their staff in information governance by carrying out the appropriate due diligence.

3. Information asset register

The DPO will advise the Trust in developing and maintaining an Information Asset Register (IAR). The register will include the following information for each asset:

- an individual information asset identification name or number.
- the owner of the asset (who is responsible for managing it).
- description and purpose of the asset.
- format and location of the asset.
- whether there is a privacy notice published for that asset.
- which employee roles/teams have routine access to the information.
- retention period for the asset.
- lawful basis for processing.
- where any data has been shared with any other data controllers.
- where the data has been shared with any third-party data processors contracted to process information through a data processing agreement.
- existence of any automated decision-making, profiling or data matching (if applicable).

The IAR will be reviewed annually and the Headteacher will be responsible for informing the DPO of any significant changes to their information assets as soon as possible.

4. Privacy notices

The Trust will provide a privacy notice to data subjects each time it obtains information from or about that data subject.

The privacy notice supplied to individuals in regard to the processing of their personal data will be written in clear, plain language which is concise and transparent.

The following privacy notices will be in place as a minimum:

- privacy notice for pupils, parents, carers.
- privacy notice for applicants.
- privacy notice for staff.
- privacy notice for Members/Trustees/SPRB members.
- privacy notice for volunteers.

All privacy notices will be displayed on the Trust and each school's individual website in an easily accessible area.

This notice will also be provided in a hard copy to pupils and parents at the start of the year as part of their information pack.

All other privacy notices stated above will be provided on application, or appointment to the Trust.

Other specific privacy notices will be issued where the data subject requires more information about specific processing.

5. Consent

The Trust will seek a positive indication of consent prior to processing any data which cannot be done so under any other lawful basis, such as complying with a regulatory requirement.

The Trust will retain records where consent is given.

The Trust will put in place arrangements for data subjects to withdraw their consent at any time.

Where a child is under the age of 16 [or younger if the law provides it (up to the age of 13)], the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

Consent will only be gained from pupils where they request it and it is deemed that the pupil has a sound understanding of what they are consenting to.

6. Information sharing and third-party processors

Information sharing

To fulfil its duty of education provision the Trust may be required share information with third parties. Routine and regular information sharing arrangements will be documented in the main privacy notices detailed in Section 4 of this policy. Any ad-hoc sharing of information will be done in compliance with our legislative requirements.

Third party processors

All third-party contractors who process data on behalf of the Trust must be able to provide assurance that they have adequate data protection controls in place to ensure that the data they process is afforded the appropriate safeguards.

Where personal data is being processed, there will be a written contract in place with the necessary data protection clauses in contained.

The Executive Leadership Team may determine that any data processing by a third party ceases immediately if it considers that the third party has not got adequate data protection safeguards in place.

If any data processing is going to take place outside the European Economic Area (EEA) then the DPO must be consulted prior to any contracts being agreed.

7. Requests for information under UK GDPR – subject access requests

Individuals have the right to obtain confirmation that their data is being processed. They also have the right to submit a subject access request (SAR) (Appendix 2) to gain access to their personal data and verify the lawfulness of processing.

Any individual appointed by the Trust as a member/trustee/SPRB member or employee may receive a request for an individual's personal information.

In all instances these requests should be immediately forwarded to the Head of Governance who will manage the SAR response process and liaise with the DPO if required.

Whilst the UK GDPR does not require such requests to be made in writing, applicants are encouraged where possible to do so.

Requests will be logged on the central Trust register and acknowledged within 5 school working days.

The Trust will take the necessary measures to validate the identity of the requester through asking for additional information such as:

- Valid Photo ID (driving license, passport).
- Proof of address (utility bill, council tax letter).
- Further information for the Trust to be satisfied of the requester's identity.
- The successful identification of a subject will be recorded on the consent form and this saved in the SAR directory on the Trust shared drive.

Once the Trust is satisfied of the requester's identity and has been provided enough information on which to respond to the request it will be considered valid. The request will then be responded to within the statutory timescale of one calendar month.

The Trust can apply a discretionary extension of up to a further two calendar months (i.e. three months in total) if the requested information would take a considerable amount of time to collate, redact, and prepare for disclosure due to either the complexity or voluminous nature of the records. The Trust will seek guidance from the DPO in these circumstances prior to informing the requester. The extension period will be kept to a minimum and will not be used as a way of managing workloads.

In very limited cases where a request is deemed manifestly unfounded or excessive, the Trust holds the right to refuse to respond to the request. This would be the case if responding would involve an unjustified amount of time and resource to comply. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal. The Trust will seek guidance from the DPO where it considers that any exemptions are necessary to apply.

If a subject access request is made by a parent of a child who is 12 years of age or over, the Trust may consult with the pupil/student or ask that they submit the request on their own behalf. This decision will be made based on the capacity and maturity of the pupil/student in question.

A copy of the information following a subject access request will be supplied to the individual free of charge. A copy of information held within a pupil's education record may incur a charge at the Trust's discretion.

Where the police request personal information, a data protection form needs to be completed. The Trust should be in receipt of a data protection form signed by a superior of the requester before processing. This form should be scanned and kept within the subject access file. An individual employee may release personal information to the police in such cases where a subject may suffer significant injury or harm should the information be withheld. This would be a personal decision by the employee and should only be made in exceptional cases when a subject is in significant danger, an example being imminent suicide.

8. Data subject rights

Data subjects have a series of rights in addition to their right to access information. These include:

- right to rectification.
- right to erasure.
- right to restrict processing.
- rights to data portability.
- rights in relation to automated decision making and profiling.

All requests exercising these rights must be in writing and forwarded to dpo@patrust.org.uk who will acknowledge the request and respond within one calendar month. Advice regarding such requests will be sought from the DPO.

A record of decisions made in respect of the request will be retained, recording details of the request, whether any information has been changed, and the reasoning for the decision made.

9. Privacy by design & privacy impact assessments

The Trust will act in accordance with the UK GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy.

The DPO will be consulted at the start of a project and will advise whether a DPIA is required. If it is agreed that a DPIA will be necessary then the DPO will assist with the completion of the assessment, providing the relevant advice.

A DPIA will usually be required in advance of introducing new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

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

- systematic and extensive processing activities, such as profiling.
- large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences.
- the use of CCTV.

Where a DPIA indicates high risk data processing, the DPO may be required to consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

10. Requests for information – Freedom of Information Act 2000 & Environmental Information Regulations 2004

Requests process

Requests for Information in accordance with the Freedom of Information Act 2000 or the Environmental Information Regulations should be made either by emailing dpo@patrust.org.uk or in writing to FOI Request, Pontefract Academies Trust, c/o Barracks Business Centre, Wakefield Road, Pontefract, WF8 4HH. Responses to all requests will be managed by the Head of Governance who will be responsible for:

- identifying whether the requested information is held.
- locating it, retrieving it or extracting the information.
- considering whether any exemption might apply, and the balance of the public interest test.
- preparing the material for disclosure and drafting the response.
- seeking any necessary approval for the response.
- sending the response to the requester.

The Trust will only accept a request for information which meets all the following criteria:

- it is in writing.
- it states the name of the applicant and the address for correspondence.
- it describes the information requested.

The Trust will not consider requests which require it to click on electronic links.

Environmental Information Regulation requests can be made verbally, however, the Trust will endeavor to follow this up in writing with the requester to ensure accuracy.

Each request received will be acknowledged within 5 school working days. The DPO will be consulted on all requests where a public interest test is applied or where there is any doubt on whether an exemption should be applied. In applying the public interest test document clearly:

- the benefits of both disclosing or withholding the requested information.
- where necessary seek guidance from previous case law in deciding where the balance lies.

The CEO will give final approval for the disclosure or non-disclosure of information where a public interest test has been applied.

The Trust will respond to the request within 20 school working days.

The Trust will not comply with the copyright section of this policy where:

- the Trust reasonably requires further information to meet a freedom of information request, has informed the applicant of this requirement, but was not subsequently supplied with that further information.
- the information is no longer readily available as it is contained in files that have been placed in archive storage or is difficult to access for similar reasons.
- a request for information is exempt under Section 2 of the Freedom of Information Act 2000.
- the cost of providing the information exceeds the appropriate limit.
- the request is vexatious.
- the request is a repeated request from the same person made within 60 consecutive days of the initial one.
- a fee notice was not honoured.

The Trust will not comply with any freedom of information request that exceeds the statutorily imposed appropriate limit of £450. When determining whether the cost of complying with a freedom of information request is within the appropriate limit, the Trust will take account only of the costs it reasonably expects to incur in relation to:

- determining whether it holds the information.
- locating the information, or a document which may contain the information.
- retrieving the information, or a document which may contain the information.
- extracting the information from a document containing it.

The Trust may, within 20 school working days, give an applicant who has requested information from the Trust, a written notice stating that a fee is to be charged for the Trust's compliance.

Charges may be made for disbursements, such as the following:

- photocopying.
- postage and packaging.
- costs directly incurred as a result of viewing information.

Fees charged will not exceed the total cost to the school of:

- informing the person making the request whether we hold the information.
- communicating the information to the person making the request.

Where a fee is to be charged, the Trust will not comply with section 11 of this policy unless the requested fee is paid within a period of three months, beginning with the day on which the fees notice is given to the applicant.

The Trust will not consider any costs which are attributable to the time spent by persons undertaking any of the activities mentioned above.

When calculating the 20th school working day in which to respond to a freedom of information request, the period beginning the day on which the fee notice is given to the applicant and ending with the day on which the fee is received, will be disregarded.

Publication of information

The Trust publishes in accordance with the publication scheme attached as **Appendix 1** to this policy and publishes as much information as possible on the Trust and school websites as appropriate in the interests of transparency and accountability.

Copyright

The Trust will take reasonable steps to inform enquirers if any third party might have a copyright or intellectual property interest in information provided in response to their requests. However, it will be the enquirer's responsibility to ensure that any information provided by the Trust is not re-used in a way which infringes those interests, whether or not any such warning was given.

Record retention and disposal

Retention periods will be determined by any legal requirement, best practice or national guidance, and lastly by the organisational necessity to retain the information. The Trust record management policy and procedures set out the Trust's arrangements.

11. Information security

Access to systems

Each school will maintain control over access to the personal data that it processes. These controls will differ depending on the format of the data and the status of the individual accessing the data. The school will maintain an audit log detailing which individuals have access to which systems (both electronic and manual). The School Support Manager or Office Manager will be responsible for ensuring that the log is maintained at all times.

Access to manual filing systems (i.e. non-electronic systems) will be controlled by a key management system. All files, that contain personal data, will be locked away in lockable storage units, such as a filing cabinet or a document safe, when not in use.

Keys to storage units will be restricted to individuals who require them to carry out legitimate business functions.

Access to electronic systems will be controlled through a system of user authentication. Individuals will be given access to electronic filing systems if required to carry out legitimate functions. All electronic systems require authentication by username and unique password.

The Headteacher will be required to inform the IT provider if any user names require suspending when an individual is on long term absence or other relevant HR matter.

New/leaving employees will be informed to the IT provider by the school (Office Manager, School Support Manager or Headteacher) or by a member of the ELT for central trust employees.

The clerk to the Trust Board will be required to inform the IT provider of new/leaving members, trustees, or SPRB members.

Individuals will be required to change their password every 90 days and will meet the following complexity requirements: Be at least eight characters in length Contain characters from three of the following four categories: uppercase letters, lowercase letters, numbers from 0 to 9, non-alphabetic/numeric characters (e g.! $, #, %).

The Trust will require that all software and system specifications which process personal information have inbuilt audit logs so that it can monitor what employees and users have accessed systems and what changes may have been made. Although this is not a preventative measure it does ensure that the integrity of the data can be assured and deters individuals from access to records without authorisation.

On occasions the Trust may need to allow individuals, who are not employees of the Trust, to have access to data systems. This could be, but not exclusively for audit purposes, to fulfil an inspection, consultants, agency/supply staff, or trainees. The Headteacher is required to authorise all instances of third parties having access to systems. If the Headteacher is not available to authorise access, then access can also be authorised by their deputy or assistant. The Director of Operations can authorise access to central trust systems or trust wide systems.
In all instances the Headteacher, their deputy or assistant or Head of Governance must ensure that the external party is made aware of this policy and their responsibilities regarding information governance and confidentiality.

An access log, detailing who has been given access to what systems and who authorised the access, will be maintained by the School/Trust.

Physical security

The Trust will maintain high standards of physical security to prevent unauthorised access to personal data. The following controls will be maintained by the Trust.

Clear desk and screen policy

Individuals will not leave personal data on desks, or in any working areas, unattended and will use the lockable storage units provided to secure personal data when not in use.

Unattended computer terminals must be turned off or locked when unattended. An auto-lock system will be invoked after a period of 20 minutes of inactivity.

Alarm system

All Trust premises will maintain security alarm systems to ensure that an adequate level of security is in operation when premises are unoccupied.

Building access

External doors to the all Trust premises will be locked when the premises are not occupied. Only authorised employees will be key holders for building premises. The Headteacher will be responsible for authorising key distribution for their school and will maintain a log of key holders.

Internal access

Internal areas which have restricted access will be kept locked and only accessed through pin pads, fobs or keys.

Visitor control

Visitors to each school will be required to sign the visitor book or on the visitor management system. Visitors will not be permitted access to restricted areas without employee supervision.

Environmental security

As well as maintaining high standards of physical security, to protect against unauthorised access to personal data, the Trust must also protect data against environmental and natural hazards such as power loss, fire, and floods.

It is accepted that these hazards may be beyond the control of the Trust, however, the Trust will implement the following mitigating controls.

Access to servers

Access to servers will be restricted as far as is practicably possible.

Back ups

Each primary school server will be backed up at least twice a week to an encrypted disk, which will be stored off site with a designated officer, a secondary disk stored in the school safe. In addition to this a weekly offsite backup is also to a secure network attached storage device located at The Kings School. This is performed over the trust wide area network (WAN).

Secondary school servers have daily backups of all crucial virtual servers which are saved to a secure network attached storage device located within a physically separate building to the core infrastructure (technology block at Carleton High School & old caretaker's house at The Kings School). A single backup is replicated weekly between these two devices ensure each school has an offsite backup.

Should the school's electronic system be compromised by an environmental or natural hazard then the school will be able to reinstate the data from the back up with minimal destruction.

The MIS (pupil management information system), the HR system and the payroll system are cloud-based systems and are backed up in accordance with the software agreement.

The Trust financial system PS Financials is held on a dedicated server located at The Kings School and is backed up daily on the cloud, it is also replicated daily to a secondary server located at Carleton High School.

Fire-proof cabinets

The Trust will aim to only purchase lockable data storage cabinets that can withstand exposure to fires for a short period of time. This will protect paper records, held in the cabinets, from any minor fires that break out on the building premises.

Fire alarm system

Each school will maintain a fire alarm system at its premises to alert individuals of potential fires and so the necessary fire protocols can be followed. The central office lease will include a fire alarm system maintained by the landlord.

Systems security

As well as physical security the Trust also protects against hazards to its IT network and electronic systems. It is recognised that the loss of, or damage to, IT systems could affect the Trust's ability to operate and could potentially endanger the lives of its pupils/students.

The Trust will implement the following systems security controls to mitigate risks to electronic systems.

Software download restrictions

Employees do not have administration rights to enable them to install software. The IT provider will only install software onto a school/central team IT system on receipt of written instruction from the Headteacher or Director of Operations. The IT provider will vet software to confirm its security certificate and ensure the software is not malicious. The IT provider will retain a list of trusted software so that this can be downloaded on to individual desktops without disruption.

Phishing emails

Each primary school server will be backed up at least twice a week to an encrypted disk, which will be stored off site with designated officer, a secondary disk stored in the school safe. In addition to this a weekly offsite backup is also to a secure network attached storage device located at The Kings School. This is performed over the trust wide area network (WAN).

Firewalls, filtering and anti-virus software

The IT provider will ensure that the Trust filtering and anti-virus software is installed on all Trust electronic devices. The IT provider will update the filtering and anti- virus software when updates are made available. The IT provider will review the Trust's filtering and anti-virus software on an annual basis and decide if they are still fit for purpose.

The Trust ISP provides a managed firewall and ensure it is configured optimally and kept up to date.

Cloud computing

The Trust currently operates its email communications on Office365. Employees will not save any other records on cloud storage unless authorised to do so by their Headteacher. This should be in limited or exceptional circumstances (i.e. google drive or one drive).

Employees are able to access email communications on their personal or work mobile telephone only if it has a pin code or bio recognition and adheres and adheres to the Office365 security policy.

Shared drives

The Trust maintains a shared drive on its servers. Whilst employees are encouraged not to store personal data on the shared drive it is recognised that on occasion there will be a genuine business requirement to do so.

The shared drive will have restricted areas that only authorised employees can access. Shared drives will still be subject to the Trust's retention schedule.

Wireless network

The IT provider will ensure that the local area networks are AES/WPA2 encrypted to the highest industry standard. WIFI passwords will be restricted to the IT providers second line support staff. The WiFi will be set up to only allow access onto the wireless network for Trust owned devices. Exceptions will only be permitted on the instruction of the CEO.

Communications security

The transmission of personal data is a key business need and, when operated securely is a benefit to the Trust and pupils/students alike. However, data transmission is extremely susceptible to unauthorised and/or malicious loss or corruption. The Trust has implemented the following transmission security controls to mitigate these risks.

Sending personal data by post

When sending personal data, excluding special category data, by post the Trust will use Royal Mail's standard postal service. Employees will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject. Envelopes should be marked "Private and Confidential, to be opened by the addressee only".

If it becomes apparent that an incorrect address has been used for correspondence which contains personal data every effort should be made to retrieve the data including collection from the delivery address.

Sending personal data and special category data by email

Where personal data is emailed to another Trust email address it is automatically encrypted and therefore secure from external interception, however all files must be password protected using passwords which are secure to the parties involved in the transaction. Where personal data is emailed external to the Trust the subject header should start with [Encrypted] to secure it from interception and requires authentication at the recipients end regardless of their system.

Special category data should only be sent externally by email in exceptional circumstances and where any other more secure means of communication is not appropriate. In such cases the instructions above will be followed and additional security of password protection will be added.

Where special category data is being sent internally by email, employees should be extra vigilant and always consider whether there is a genuine need to send the information in an email. Personal comments should never be included in emails, and care should be taken to ensure the accuracy of information. In all instances, employees must always double check the recipient's email address to ensure that the email is being sent to the intended individual(s).

Exceptional circumstances

In exceptional circumstance the Trust may wish to hand deliver, or use a direct courier, to ensure safe transmission of personal data. This could be because the personal data is so sensitive usual transmission methods would not be considered secure or because the volume of the data that needs to be transmitted is too big for usual transmission methods.

Using the BCC function

When sending emails to a large number of recipients, such as a mail shot, or when it would not be appropriate for recipients to know each other's email addresses then employees will utilise the blind copy (BCC) function.

Transferring and sharing data

All data transferred or shared should be done so securely and an appropriate written protocol or processing agreement in place.

Surveillance security

A number of Trust schools operate CCTV. Due to the sensitivity of information that could be collected as a result of this operation, the Trust has a separate policy which governs the use of CCTV.

Remote working

It is understood that on some occasion employees of the Trust will need to work at home or away from school premises. If this is the case, then employees will adhere to the following controls.

Storage security

When files or equipment are stored at home they should not be openly accessible to other members the household.

Employees must always lock their computer screen when away from their computer/laptop.

Employees must not keep personal data or school equipment unsupervised at home for extended periods of time (for example when the employee goes on holiday).

Employees must not keep personal data or school equipment in cars if unsupervised.

Private workings area

Employees must not work with personal data in areas where other individuals could potentially view or even copy the personal data (for example on public transport).

Employees should also take care to ensure that other household members do not have access to personal data and do not use school equipment for their own personal use.

Trusted WIFI connections

Employees will only connect their devices to Trust Wi-Fi connections and will not use 'free public Wi-Fi' or 'guest Wi-Fi'. This is because such connections are susceptible to malicious intrusion.

When using home Wi-Fi networks employees should ensure that they have appropriate anti-virus software and firewalls installed to safeguard against malicious intrusion. If in doubt employees should seek assistance from IT Provider.

Using home computers

Employees allocated with a device by the Trust should use this device rather than a personal device.

When an employee is using their home computer/device to access school remote services or email then they should firstly ensure that their computer is up to date with the latest anti-virus protection. Any information or files should not be downloaded to the home computer/device and should be stored on the accessible network/cloud drives allocated by the school.

The employee should not leave the device unattended and should ensure they log off all Trust systems completely at the end of any session.

If an employee has the facility to print from home then this should be limited and not stored at home. Should an employee need to print off any personal data at home, this should be kept securely away from other members of the household and disposed of as quickly as possible using an approved method within the Trust.

Employees should ensure that meetings where personal data is shared occur in a secure location within the home out of earshot or possible recording of another household member. Headphone/speaker sets will be made available to staff on request.

Where the above conditions cannot be met then the member of staff should take advice from their line manager/information champion where consideration will be given to alternative locations of work.

Disposal of data and information

Documents containing information which is confidential or includes personal data must be disposed of through cross shredding disposal or a certified UK GDPR compliant personal data shredding service. A destruction log will be completed when the final copy of personal data is destroyed. Personal data held in containers or consoles will be locked, in restricted areas with controlled access restricted to the Headteacher or collection provider.

Disposal of computer equipment must be via RM Education and should be stored in secure rooms/cabinets prior to disposal. In all instances RM Education will be responsible for making arrangement and retaining the audit log of disposal and forwarding a copy to the school.

Where MFD devices are collected at the end of the lease period, the school (for school-based devices) or central team must ensure before removal that the memory has been erased of all documents.

Disposal of data and information/intellectual property

Any information or intellectual property held or developed on trust systems or through a contract of employment or commercial contract remains the property of the Trust.

All systems must be monitored and audited for administrative, legislative and management purposes, therefore, personal privacy cannot be guaranteed.

It may be necessary to access systems and equipment during an employee's absence to ensure business continuity and compliance with the Freedom of Information Act.

12. Information security incident reporting

Definition of a breach

An information security incident is an event which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately and has caused or has the potential to cause damage to the Trust's information assets and/or reputation.

An information security incident may be confirmed or suspected. An information security incident includes, but is not restricted to:

- loss or theft of confidential or special category data, or portable equipment/paper which such data is stored/recorded.
- equipment theft or failure.
- unauthorised use, access or modification of data or information systems.
- attempts (failed or successful) to gain unauthorised access to information or IT systems.

- unauthorised disclosure of special category and confidential data.
- website defacement.
- hacking attack.
- loss as a result of fire or flood.
- human error.
- deception – obtaining or attempting to obtain information through imitation.

Notification and containment

Article 33 of the UK GDPR compels data controllers to report breaches of personal data to the Information Commissioner's Office (ICO) within 72 hours of discovery if the incident is likely to result in a risk to the rights and freedoms of data subjects. Therefore, it is vital that the Trust has a robust system in place to manage, contain, and report such incidents.

Immediate action (within 24 hours)

If an employee, trustee, SPRB member, or contractor is made aware of an actual data breach, or an information security event (a 'near miss') they must report it to their line manager, the Headteacher, and the Head of Governance within 24 hours.

If appropriate, the employee who located the breach, the line manager, or Headteacher will make every effort to retrieve the information and/or ensure recipient parties do not possess a copy of the information.

Assigning investigation (within 48 hours)

Once received the Headteacher in liaison with the Head of Governance will assess the data protection risks and assign a severity rating according to the identified risks and mitigations. The severity ratings are:

Severity	Analysis	Action Required
White	**Information security event** No breach has taken place but there is a failure of the implemented safeguarding that could cause a data breach in the future.	Log and send a reminder to employees **Examples:** • emails sent to the wrong person but does not contain personal data. • found post-it notes with username and password but has not been used for any known detriment.
Green	**Minimal Impact** A data breach has occurred but has been contained within the organisation (or trusted partner organisation), the information is not considered to be particularly sensitive, and no further action is deemed necessary.	**Conduct an internal investigation example:** • emails that contained personal data, sent to the wrong member of staff but kept within the organisation and no harm caused. • information on child's file is incorrect/mixed up.

Amber	**Moderate Impact** Security measures have failed and consequently have resulted in the loss, release, or corruption of personal data. However, the actual or potential detriment is limited in impact and does not reach the threshold for reporting to the information commissioner's office.	**Action: Conduct an internal investigation** • letter sent to the wrong parent revealing a fact about another child but not considered sensitive enough to warrant detriment. • lost information about a child's progress.
Red	**Serious Impact** A breach of security involving sensitive personal data and/or a large volume of personal data. The incident has or is likely to cause serious detriment (emotional, financial, or physical damage) to individuals concerned. The breach warrants potential reporting to the information commissioner's office and urgent remedial action. HR input may also be required.	**Action: Contact the DPO ASAP** • safeguarding information has been disclosed to the wrong parent. • lost medical information about a child (such as life-threatening allergies).

The Headteacher will notify the relevant information asset owner that the breach has taken place. The Headteacher will recommend immediate actions that need to take place to contain the incident.

The information asset owner will investigate white, green and amber incidents. Red incidents will be investigated by the data protection officer with the assistance of the Trust internal audit service and counter fraud teams as appropriate.

Reporting the breach to the ICO/data subjects (within 72 hours)

The Head of Governance and the DPO will decide as to whether the incident needs reporting to the ICO, and also whether any data subjects need to be informed. The Headteacher will be responsible for liaising with data subjects and the DPO for liaising with the ICO.

Investigation and concluding incidents

The Headteacher will ensure that all investigations have identified all potential information risks and that remedial actions have been implemented.
When the DPO has investigated a data breach relating to a specific school then the Headteacher must sign off the investigation report and ensure recommendations are implemented in their school. If a data breach relates to an incident across the Trust or in the central team then the CEO must sign off the investigation report and ensure recommendations are implemented across the Trust.

The Headteacher in liaison with the Head of Governance will ensure that all investigations have been carried out thoroughly and all highlighted information security risks addressed.

Where recommendations made following a breach in one school will improve the information culture across the Trust the Head of Governance will review procedures and liaise with information champions as appropriate.

Retaining a register of breaches

The Head of Governance will maintain a register of all information security breaches across the Trust.

13. Records management

Responsibilities

The Trust has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for implementing this policy is the Headteacher for the records in their school and the Head of Governance for records held by the Trust.

The SIRO will act as the accountable person and a champion for records management. They will oversee records management policy and strategy and ensure that the necessary resources are made available and remedial action is taken when problems arise. They will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately, and will support appropriate allocation of resources towards the school's records management programme, and will promote records management training for all staff.

The person with operational responsibility for the school's records management programme is School Support Manager (in secondary schools) and Office Manager (in primary schools). They will ensure that the programme is developed, manage its implementation and overall functioning, including the production of any school specific procedures and guidance, work with the Head of Governance to determine vital records and develop and implement disposal policies and schedules, as well as facilitating programme reviews and improvements.

All staff (including temporary staff) must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the Trust's records management guidelines.

Relationships with existing policies

This policy has been drawn up within the context of the Trust's Information Governance Policy Framework. In particular it flows from the Trust's Information Policy and helps to facilitate compliance with the requirements of the General Data Protection Regulation, Environmental Information Regulations 2004 (EIR) and Freedom of Information Act 2000 (FOIA), associated guidance and Codes of Practice issued under the legislation.

The Trust has adopted the retention schedule developed by the Information and Records Management Society (IRMS) to support its management and storage of information.

14. Surveillance

CCTV

A number of schools in the Trust operate 'Closed Circuit Television' (CCTV) systems in order to maintain security and safeguard employees and students/pupils.

Planning CCTV systems

Any new implementation of CCTV systems will employ the concept of 'privacy by design' which will ensure that privacy implications to data subjects will be considered before any new system is procured. The prescribed method for this is through the completion of a data protection impact assessment (DPIA).

The Trust has various statutory responsibilities to protect the privacy rights of data subjects. Therefore, during this planning phase, the Trust will consider:

- the purpose of the system and any risks to the privacy of data subjects.
- that there are statutory requirements placed on the location and position of cameras. This means that cameras must be positioned to meet the requirement(s) of the intended purpose(s) and not exceed the intended purpose(s).
- the obligation to ensure that the CCTV system can meet its intended purpose(s) also means that the system specification must be such that it can pick up any details required for these aims. For example, the system must record with sufficient resolution to perform its task.
- the system must also have a set retention period (the typical retention period is one month) and, where appropriate, the respective school must also have the ability to delete this information prior than the set retention period in order to comply with the rights of data subjects.
- that the specific school will need a level of access to the system and there will need to be the option to provide other agencies (such as law enforcement agencies) with specific footage if requested. If a data subject is captured and recorded by the system, then that individual also has the right to request a copy of that footage under subject access provisions.

The Trust will ensure that a contract will be agreed between the Trust (as Data Controller) and the CCTV system provider. Consideration should also be given as to whether there are any joint data controller arrangements where the system is shared with another organisation. Data processing clauses must be included within the written contract if the provider will be processing (e.g. monitoring, storing, accessing) the data on behalf of the school.

CCTV privacy notices

The processing of personal data requires that the individuals that the data relates to (in this case any individuals captured by the CCTV) are made aware of the processing. Therefore, the use of CCTV systems must be visibly signed.

The signage will include the purpose for the system (e.g. the prevention or detection of crime), the details of the organisation operating the system and who to contact about the system (including basic contact details).

The signage must be clear enough that anyone entering the recorded area will be aware that they are being recorded.

A more detailed privacy notice for the use of CCTV must be maintained with the intention of informing data subjects of their rights in relation to surveillance data.

Access to CCTV recording

CCTV footage will only be accessed to comply with the specified purpose. For example, if the purpose of maintaining a CCTV system is to prevent and detect crime then the footage must only be examined where there is evidence to suggest criminal activity having taken place.

The CCTV system will have a nominated information asset owner who will be responsible for the governance and security of the system. The information asset owner will authorise officers to access CCTV footage either routinely or on an ad-hoc basis.

CCTV footage disclosures

A request by individuals for CCTV recordings that include footage of them should be regarded as a subject access request (SAR). For more information on the right of access for individuals captured on CCTV, refer to the Trust's information policy.

If the Trust receives a request from another agency (for example a law enforcement agency) for CCTV recordings, then it will confirm the following details with that agency:

- the purpose of the request.
- that agency's lawful basis for processing the footage.
- confirmation that not receiving the information will prejudice their investigation.
- whether the Trust can inform the data subject of the disclosure, and if not, the reasons for not doing so.

The Trust will liaise with its appointed data protection officer should it have any concerns about such requests.

Review of CCTV

CCTV systems must be reviewed biennially to ensure that systems still comply with Data Protection legislation and national standards. The information asset owner should use the checklist included in **Annex 6** of this policy to complete this review. It is the responsibility of the information asset owner to ensure reviews are completed and evidence of those reviews taking place are maintained.

Complaints

Complaints by individuals about the use of surveillance systems, or the way surveillance data is processed, should be treated as a data protection concern and the school's data protection officer should be made aware of.

The school's data protection officer is:

Information Governance
Veritau Ltd
County Hall
Racecourse Lane
Northallerton
DL7 8AL
schoolsDPO@veriau.co.uk
01609 532 526

Records of processing

The Trust has a duty under Article 30 of the UK GDPR to ensure that all instances of data processing activity is recorded for regulatory inspection where required. Each school in the Trust maintains an information asset register in order to fulfil this requirement.

Each school will ensure that the use of surveillance systems is recorded on their information asset register. Each school should detail each separate surveillance system in use.

Related documents

Employees who are responsible for planning, maintaining, or reviewing the implementation of a surveillance system are encouraged to read the following related documents prior to implementation:

- ICO Surveillance Code of Practice (External Link).

Appendix A: Information Security Incident Guidance

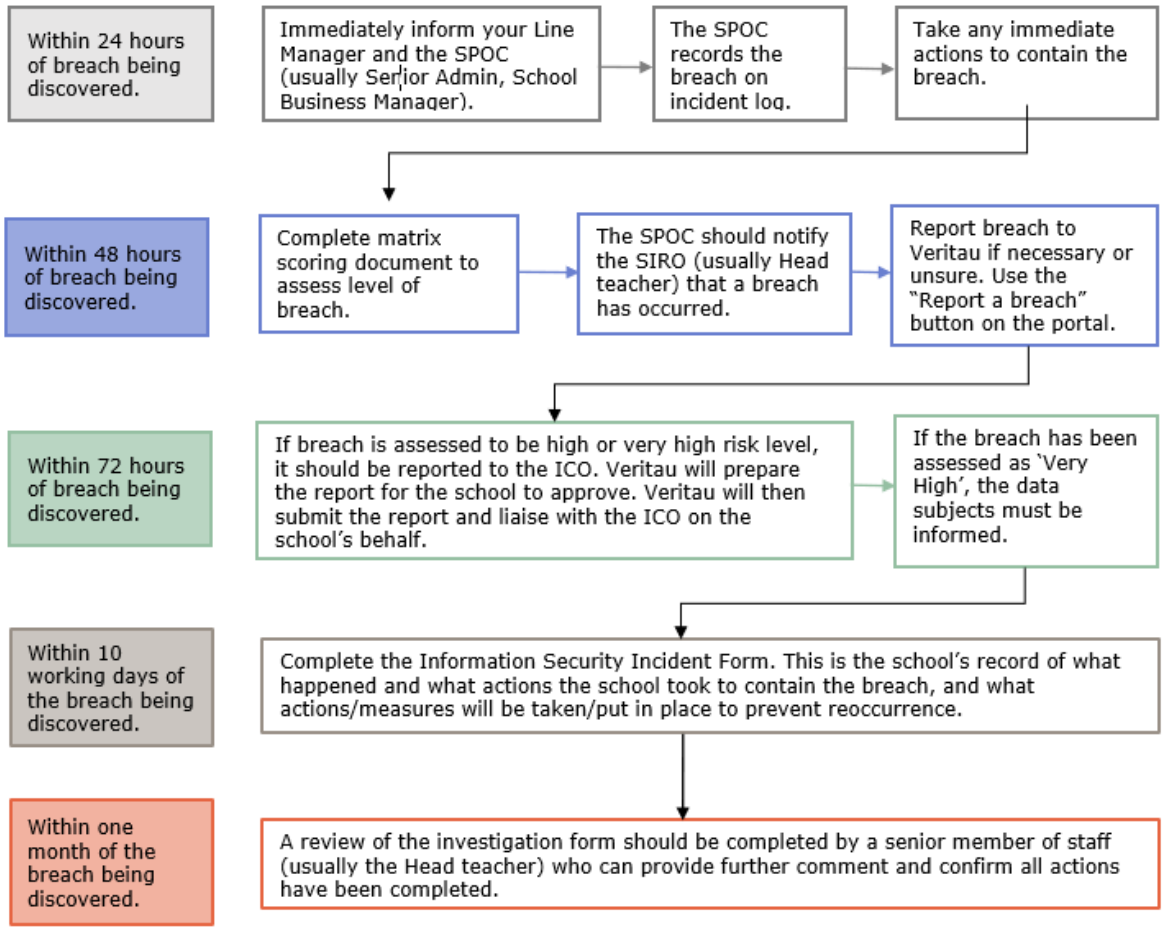
An information security incident is where unauthorised access or disclosure of information (electronic or hard copy) has occurred. If the information also contains personal data, this is also known as a 'data breach'. The severity of incidents can vary from minor to very severe, however all incidents of this type should be treated seriously. Appropriate measures should be put in place to ensure continuous improvement to information security practice, preventing minor incidents turning into major incidents.

When an incident occurs, please ensure you follow the Information Security Incident Reporting section of this policy.

This document has been produced to provide further guidance around the documentation that needs to be completed and actions to consider. In all instances, notification should be to the Head of Governance who will lead on the process.

Steps to follow

The below flow chart sums up the steps to follow should a data breach occur. Follow the Information Security Incident Reporting section of this policy and aim to complete the actions in the flow chart as per below timescales.



Information Security Incident Form

Any information security incident must be recorded in a logical and concise manner. It is important that should the incident involve personal data and a report be required for the ICO we are able to submit all the relevant detail to them.

The form may look to be a long and complicated document, but it has been designed to enable you to capture the information quickly and efficiently you need to, with most prompts requiring you to select the correct statement.

The form is divided into four stages that cover the full life cycle of an incident.

Stage 1 – initial recording and reporting of the incident

- Part 1 covers when, who and by whom the incident is first discovered, how it was reported and recorded. If any initial steps were taken to prevent further disclose or loss and which staff members are involved in the incident.
- Part 2 records the details of any personal data that was involved in the incident.

NB: If there was no personal data involved this section can be skipped and you can move to Stage 3.

Stage 2 – completion of the initial risk assessment for a personal data breach
To assess the risk to individuals (data subjects) because of a data breach. Further details on this are outlined below.

Stage 3 – investigation of the incident
To review of what controls are currently in place at the school to protect all data. These can be both physical and technical security steps. Assess how they are supported by appropriate processes and policies and that staff are adequately trained in what they are expected to do. There is also an action plan to identify what can be implemented to prevent such an incident happening again.

Stage 4 – review of the incident
This only applies to high/very high breaches. The SIRO is required to review the incident and confirm that the agreed actions have been completed. There is also a section for the involvement of the Executive Leadership Team/SPRB Members/Trustees in this final review stage where there has been a particularly severe incident. This is optional, and dependent on the role they play in the school.

How to identify risk scores for the Incident Form

The risk assessment scoring matrix has been designed to be easy to use and will provide a clear conclusion as to what the next steps must be to remain compliant.

Using the matrix assesses the risk to the rights and freedoms of individuals affected by the data breach and will assist with deciding if the data breach should be notified to those affected and/or whether a formal report to the ICO is required.

The matrix covers the areas of sensitivity of the data, the potential impact to the individual and the likelihood that the adverse impact may occur.

Risk Ratings

By working your way through the risk assessment scoring matrix, noting the weighting given to each response given you will be able to produce a total sum of all tables at the end of the assessment. This total can then be aligned to the risk level categorised in the table.

Each risk level indicates whether notification to the individual or/and the ICO may be required, but please do speak to Veritau for our advice and recommendation.

Very Low/Low Risk
These do not need reporting to Veritau. How the incident occurred and what steps need to be taken to prevent similar breaches happening again should be considered and recorded. It would also be useful for such incidents to be used as learning tools in staff training.

Moderate/High/Very High Risk
Contact the DPO team at Veritau for them to make a judgement as to whether we need to conduct an investigation and if the incident needs reporting to the Information Commissioner's Office (ICO). Reporting of severe incidents is a legal requirement and must be done within 72 hours of becoming aware of the breach (including evenings and weekends). If in doubt, please call us for advice.

Notifying Individuals

The risk assessment matrix you completed will help form your decision on whether data subjects should be notified of the breach. However, there are also some additional considerations:

- Is the breach of their data sufficiently serious enough to warrant telling them, or will more harm be caused by informing them? E.g. could it worsen their mental health?

- Are there any other circumstances that would encourage you to inform the data subject even if by law you don't have to?

  For example, is the breach in the public domain or on social media? Are other parents/pupils already aware of the breach?

  The school wants to maintain a positive relationship with pupils/parents through being transparent. If the data subject were to be informed via other means it could damage the relationship and have an impact on the school's ability to provide adequate education provision.

Key points to remember

- Ensure you have robust information security policies and measures in place.

For example, do not to store documents containing personal data on an unencrypted memory stick, except briefly for transportation.

- When considering why an incident occurred, try to think beyond 'human error'.

  There will usually be an underlying reason why the error was made, such as overworking, lack of training, lack of information security measures etc. Consideration of this will lead to improved information security practice and a less stressful working environment when handling information.

- Please do not panic! Although all incidents need to be taken seriously, it is important to handle the incident in a calm and collected manner.

Examples

There are many information security incidents that can and do occur. Below is a small number of examples to give you an indication of severity levels.

1) **A parent notifies you that they have been sent the wrong child's progress report.**
   Providing the workbook does not contain any sensitive information (for example, that the child has a particular medical condition affecting his/her work), this is a fairly minor security incident with a **low risk** level.

2) **An email is received from another school in the local authority containing an attendance record for a whole year group. It contains medical data as it details the reasons for absence.**
   This is a **moderate** information security incident. Although the information has left the school's control and contains medical data, the risk is low as the information has gone to another local authority school and is therefore not in the public domain.

3) **A spreadsheet containing the SEN information for all the School's pupils has been mistakenly sent to a member of the public.**
   This is a very severe security incident due to the potentially catastrophic impact on the children and as a **high risk** level would need reporting immediately.

*Please note that the severity of the above examples can be completely different depending on slight changes of facts/type of information therefore it is important to stress that the severity of incidents should be considered on a case-by-case basis***.**

Appendix B: Freedom of information publication scheme

Information to be published	How the information can be obtained (hard copy and/or website)	Cost
Class 1 – who we are and what we do		
Who's who in the Trust and its schools	Trust website School websites	Free
Who's who on the members/Trust Board/School Performance Review Boards	Trust website School websites	Free
Instrument of Government/Articles of Association/Funding Agreement	Trust website	Free
Contact details for the CEO, Headteacher and for the Trust Board, School Performance Review Boards via the Trust/schools (named contacts where possible)	Trust website School websites	Free
School prospectus (if any)	School websites	Free
Staffing structure	Trust website School websites	Free
School session times and term dates	School websites	Free
Address of school and contact details, including email address	Trust website School websites	Free
Class 2 – what we spend and how we spend it		
Annual budget plan Annual report and financial statements	Hard copy Trust website	Free
Capital funding	Hard copy	Free
Financial Audit reports	Hard copy	10p/sheet
Procurement and contracts the Trust has entered into, or information relating to/a link to information held by an organisation which has done so on its behalf (for example a local authority or diocese).	Hard copy	10p/sheet
Pay policy	Trust website	Free
Class 3 – what our priorities are and how we are doing		
School profile Performance data supplied to the English Government, or a direct link to the data The latest Ofsted reports Post-inspection action plan	School website School website School website Hard copy	Free
Performance management policy and procedures.	Trust website	Free
Performance data or a direct link to it	Trust website School websites	Free Free
The school's future plans; for example, proposals for and any consultation on the future of the school, such as a change in status	Trust website School websites	Free Free
Safeguarding and child protection	School websites	Free
Class 4 – how we make decisions		
Admissions policy/decisions (not individual admission decisions) – where applicable	Trust website School websites	Free
Agendas and minutes of meetings of the Trust Board and its committees	Hard copy	10p/sheet

(NB this will exclude information that is properly regarded as private to the meetings)		
Class 5 – Our policies and procedures		
Governance Policies Finance Policies HR Policies Health and Safety at Work Policies Records management and personal data policies, including: • Information security policies • Records retention, destruction, and archive policies Data protection (including information sharing policies)	Trust website School websites	Free
Charging regimes and policies	School websites	Free
Class 6 – Lists and registers		
Curriculum circulars and statutory instruments	Hard copy	Free
Any information the school is currently legally required to hold in publicly available registers *(this does not include the attendance register)*	Hard copy	10p/sheet
Class 7 – the services we offer		
Extra-curricular activities	School websites	Free
Out of school clubs	School websites	Free
Services for which the school is entitled to recover a fee, together with those fees	Hard copy	10p/sheet
Additional information		
Subject access requests	Hard copy of electronic	No charge

Schedule of charges

This describes how the charges have been arrived at:

Type of charge	Description	Basis of charge
Disbursement cost	Photocopying/printing @ 10p per sheet (black & white)	Actual cost*
	Postage	Actual costs of Royal Mal standard 2nd class

*the actual cost incurred by the Trust

Appendix C: Subject access request

Subject access request form

1. Details of person requesting the information:

Name of requestee:	
Current address:	
Postcode:	
Telephone number:	
Email address:	

2. Proof of identity:

To establish your identity and address, this application must be accompanied by an original or a photocopy document(s) bearing your fill name (first name(s) and last name), date of birth and address (e.g. driving licence). Any original identification documents will be returned; photocopies of identification documents will be destroyed after they have been checked.

I can confirm I have attached the following photocopy to this form (please select one of the below options):

a. Passport
b. Driving licence
c. Utility bill
d. Council tax letter

3. Written authority of applicant

If you are acting on behalf of a data subject who is 13 or over (i.e. the person to whom the information is about), their written authority is required. Please complete the details below. Please also state your relationship to the data subject (e.g. solicitor, client, parent, child etc.)

Your full name	
Current address	
Postcode	
Tel no	
Email address	
Relationship to applicant	
Signature	

4. Information required

Please detail what information you require, providing as much information as possible:

Please specify the name of the school:	

5. Declaration (to be signed by the applicant)

I certify the information given on this application form to Pontefract Academies Trust is true. I understand that it is necessary for PAT to confirm my/data subject's identity and it may be necessary to obtain more detailed information in order to locate the correct information.

Full name (including title):	
Signature:	
Date:	

6. Please send your completed form with a copy of your ID attached to:

Subject Access Request
Pontefract Academies Trust
The Barracks Business Centre
Wakefield Road, Pontefract
WF8 4HH

or via email to DPO@patrust.org.uk

Appendix D: Schedule of environment security measures

School	Server Location	Back Up location
Carleton High School	Annex Block – locked room	Technology Block (automatic)
The King's School	ICT/Maths Block - locked room	Caretakers House (automatic)
Carleton Park	Admin Office	Disks held in the school safe *(designated officer responsible for disk rotation)*
De Lacy Primary	Server Room	Disks held in the school safe. *(designated officer responsible for disk rotation)*
Halfpenny Lane	Locked Cupboard	Disks held in the school safe. *(designated officer responsible for disk rotation)*
Larks Hill	Secure cabinet in ICT suite	Disks held in the school safe. *(designated officer responsible for disk rotation)*
Orchard Head	Server Room	Disks held in the school safe. *(designated officer responsible for disk rotation)*
The Rookeries	Old Admin Office	Disks held in the school safe. *(designated officer responsible for disk rotation)*
Central Team	Server Room – locked room	Stored on the King's School Server configuration

Firewalls are managed by RM Education.

Anti-virus software licence renewal is managed by RM Education and is currently provided by Sophos.

Filtering software licence renewal is managed by RM Education and is currently provided by Censornet.

Appendix E: Information Security Incident Reporting and Investigation Form

Do not provide personal details of those involved or affected by a data breach. E.g. refer to them as pupils, service users, parents etc.

Stage 1: Initial recording and reporting of the incident

Serious breaches should be reported to Veritau within 24 hours of discovery.

You should use this report to record your breach in full. This is available on the Schools Portal and Veritau can assist with completing it.

Parts 1 and 2 of this report form the part of Veritau's "report a breach" function on the portal. So if you have used that function to report a breach to Veritau, you will have already completed these parts and your answers can just be pasted in to the relevant boxes below. You will then need to complete the rest of the boxes in this report to ensure the school has a full record of the breach and all actions taken.

Part 1 - About the incident	
Date and time the incident occurred	
Date and time the school became aware of the incident	
How did you first become aware of the incident? (e.g. reported by a staff member, parent or pupil)	
Who has the incident been reported to? (name and position at the school, or external organisations such as your IT team or the police)	
Incident reference number (if applicable for your school)	
Description of the incident Please provide as much detail and write as clearly as possible, including: • Who was involved and advised (job titles) • The cause of the breach (e.g. high workload, distracting workspace, new system, lack of training) • Explanation of any delay in reporting the incident	
Initial response by the school Provide details of any immediate actions that you have taken (e.g. removed published data, requested deletion of an email, password changes on systems, theft of equipment reported to the police).	
Have you been able to recover the personal data (if applicable)?	

Part 1 - About the incident	
Provide details e.g. you have retrieved a letter sent to the wrong parent etc.	
Have you informed the data subject(s)? This is the person the information relates to. If you have informed them please briefly describe their reaction (e.g. are they very concerned? Did they express any particular worries?).	

Part 2 – About the personal data	
How many individuals did the breached data relate to?	
Are there other people who may also be affected by the breach of the personal data? If so, how many? (E.g. parents of the pupils, family of a teacher etc.?)	
Categories of individuals affected Select all that apply	Employees ☐ Pupils ☐ Parents ☐ Other (please give details below): ☐ Click or tap here to enter text.
Does the information disclosed contain data that could identify the individuals? Select all those that apply	Name ☐ DOB ☐ Contact details ☐ Location data ☐ Online identifiers such as IP address and cookie identifiers ☐ Identification data such as usernames or passwords ☐ Official documents (e.g. passport) ☐ Free school meal status ☐ Other (please give details below): ☐ Click or tap here to enter text.
Does the data contain any sensitive or special category data? Select all that apply	Racial or ethnic origin ☐ Political opinions ☐ Religious or philosophical beliefs ☐ Trade union membership ☐ Genetic data ☐ Biometric data ☐ Health data (including SEN info) ☐ Data regarding sex life or orientation ☐ Criminal offence data ☐ Safeguarding information ☐

Part 2 – About the personal data		
	Financial information (bank details, credit card numbers, any information indicating financial status)	☐
Are there any other details which should be noted? e.g. any additional risks which could increase the harm/detriment to individuals involved or affect the investigation in any way.		

Stage 2: Risk assessment scoring

Please use the risk matrix scoring form and add the score and risk level to the box below.

Risk Score from Matrix (totals from all tables)	

Decision to inform data subjects/individuals affected

Reportable to individuals from the Matrix? Please select.	**NO**
Are there additional factors to consider regarding notifying individuals? Provide your reasoning and if specialist advice was required.	
Final decision to inform	Choose an item.
Decision makers details	
Date	Click or tap to enter a date.

Decision to inform ICO (made in conjunction with the DPO)

Reportable to ICO from the matrix? Please select.	**NO**
Are there additional factors to consider regarding notification? Provide your reasoning and if specialist advice was required.	
Final decision to inform	Choose an item.
Decision makers details	
Date	Click or tap to enter a date.
DPO details	
Date	Click or tap to enter a date.

Stage 3: Investigation

Understanding what data security measures are currently in place This section is about the internal controls that the school has in place to protect all data it holds across its systems, both electronically and physical files.

Provide details of any relevant measures you already had in place to prevent a breach of this type occurring. For example: • Details of staff training, • What policies , processes and procedures are used within the school • Security controls in place (both physical – locked storage etc. and technical – passwords, encryption etc.).	
Are there relevant policies, procedures or guidance that set out what should have happened. If so what are they?	
Were the above appropriate security guidelines being followed? If not explain why.	
Has this type of incident occurred at the school before? If so, provide please a brief summary of • The date when it happened, • Who was involved in the incident (job titles) What the outcome of the investigation was (E.g. was any additional security or training put in place?)	

Training and communication This section is about whether staff understood what organisational and technical data security measures were in place	
If a member of staff was involved in the personal data breach, have they received data protection training within the last two years? (Please confirm what training has been completed)	
What evidence is there to communicate the process to be followed? (E.g. email reminders or staff meeting discussions)	
Was the training/communications provided being followed? If not explain why.	

Other factors for consideration	
Please provide any other factors that should be taken into consideration relating to the security incident. (E.g. the use of autocomplete for email addresses meant the wrong email address was selected)	

What was the root cause? (E.g. a change in working conditions, working from home, higher workload, staff absence, a lack of appropriate equipment, technology issues, lack of secure storage)	

Action Plan

This section is where you identify any improvements to reduce the risk of reoccurrence. This is also the place to record how lessons learned can be shared with colleagues. You can attach any documentary evidence to support the actions to this incident report.

	Identified area for improvement	Action required	By whom?	Date completed
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Appendix F: Retention schedule

1.	Trustees / SPRB members				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
1.1	Register of Members, Membership Certificates	No	Companies Act 2006	Permanent	Secure disposal
1.2	Register of Trustees, declaration of willingness and eligibility to act as a Director	No	Companies Act 2006	Permanent	Secure disposal
1.3	Minutes (Members, Trustees, SPRB members)	There may be data protection issues if the meeting is dealing with confidential issues relating to staff	Companies Act 2006	Permanent	If the school is unable to store these then the archives service should be used.
	Trust/School set (signed)				
	Inspection Copies	No		Date of meeting + 3 years	Secure disposal
1.4	Agendas (Members, Trustees, SPRB members)	There may be data protection issues if	Companies Act 2006	Date of meeting + 10 Years (One master copy retained with signed minutes)	Secure disposal

1.	Trustees / SPRB members				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
		the meeting is dealing with confidential issues relating to staff			
1.5	Reports (Members, Trustees, SPRB members)	There may be data protection issues if the report deals with confidential issues relating to staff	Companies Act 2006	Reports should be kept for a minimum of 10 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently	Secure disposal
1.6	Meeting papers relating to the annual parents' meeting held under section 33 of the Education Act 2002	No	Education Act 2002, Section 33	Date of report + 6 years	Secure disposal
1.7	Instruments of government including the Memorandum and Articles of Association	No		Permanent	Retain whilst school open
1.8	Trust and endowments	No		Permanent	Retain whilst operationally required
1.9	Action plans created and administered	No		Expiry of Plan + 3 years	Secure disposal

1.	Trustees / SPRB members				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
	by the Trust Board and/or school performance review boards				
1.10	Policy documents created and administered by the Trust Board and/or school performance review board	No		Expiry of Policy + 3 years	Secure disposal
1.11	Records relating to complaints dealt with by the Trust Board or school performance review board	Yes		Date of resolution of complaint + 6 years. After six years review for further retention in the case of contentious disputes.	Secure disposal
1.13	Signed business interest forms	No	Companies Act 2006	Permanent	Secure disposal
1.14	Signed gifts and hospitality forms	No	Companies Act 2006	Permanent	Secure disposal
1.15	EFA approvals	No	Funding Agreement	Permanent	Secure disposal

2.	CEO, Executive Headteacher, Headteacher, Senior Leadership Teams				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
2.1	Log books of activity in the school maintained by the Headteacher	There may be data protection issues if the log		Date of last entry in the book + a minimum of 6 years then review	These could be of permanent historical value and should be offered to the County Archives

		book refers to individual pupils or members of staff			Service if appropriate
2.2	Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff		Date of the meeting + 3 years then review	Secure disposal
2.3	Reports created by the Head Teacher or the Management Team	There may be data protection issues if the report refers to individual pupils or members of staff		Date of the report + a minimum of 3 years then review	Secure disposal
2.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the records		Current academic year + 6 years then review	Secure disposal

		refer to individual pupils or members of staff			
2.5	Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the records refer to individual pupils or members of staff		Date of correspondence + 3 years then review	Secure disposal
2.6	Professional Development Plans	Yes		Life of the plan + 6 years	Secure disposal
2.7	School development plans	No		Life of the plan + 3 years	Secure disposal

3.	**Property and insurance**				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
3.1	Title deeds	No		Permanent	
3.2	Plans	No		Permanent	
3.3	Planning permission	No		Permanent	
3.4	Maintenance and contractors	No		Current year + 6 years	Secure disposal
3.5	Lease register and leases	No		Expiry of lease + 6 years	Secure disposal

3.	Property and insurance				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
3.6	Lettings diary and receipts	Yes		Current year + 3 years	Secure disposal
3.7	Burglary, theft, vandalism report forms	Yes		Current year + 6 years	Secure disposal

4.	Finance				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
4.1	Annual report and financial statements	No		Current year + 6 years	Standard disposal
4.2	Loans and grants	No		Date of last payment on loan + 12 years then review	Secure disposal
4.3	Contract				
	Under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	Secure disposal
	Under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	Secure disposal
	Monitoring records	No		Current year + 2 years	Secure disposal
	Register	No		Include all current plus those completed within last 6 years	Secure disposal
4.4	Orders & requisitions	No		Current year + 6 years	Secure disposal
4.5	Copy remittances	No		Current year + 6 years	Secure disposal
4.6	Receipt books	No		Current year + 6 years	Secure disposal

4.	Finance				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
4.7	Budget reports, budget monitoring	Possible		Life of the budget + 3 years	Secure disposal
4.8	Invoices	No		Current year + 6 years	Secure disposal
4.9	Delivery / goods received notes	No		Current year + 6 years	Secure disposal
4.10	Debtor records	No		Current year + 6 years	Secure disposal
4.11	Cheque books	No		Current year + 6 years	Secure disposal
4.12	Paying in books	No		Current year + 6 years	Secure disposal
4.13	Petty cash books	No		Current year + 6 years	Secure disposal
4.14	Signed bank reconciliations	No		Current year + 6 years	Secure disposal
4.15	Bank statements	No		Current year + 6 years	Secure disposal
4.16	Grant claims	No		Current year + 6 years	Secure disposal
4.17	Consultants – diary of visits, reports generated	No		Current year + 6 years	Secure disposal
4.18	Donations register	No		Current year + 6 years	Secure disposal
4.19	Free school meal registers	No		Current year + 6 year	Secure disposal
4.20	School meal registers and summaries	No		Current year + 6 year	Secure disposal

5.	Recruitment				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
5.1	All records leading up to the appointment of a new headteacher	Yes		Date of appointment + 6 years	Secure disposal
5.2	All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	Secure disposal
5.3	All records leading up to the appointment of a new member of staff – successful candidate	Yes		6 years from the end of employment	Secure disposal
5.4	Pre-employment vetting information – DBS Checks	No	DBS Update Service Employer Guide June 2014: Keeping children safe in education July 2015 (Statutory Guidance from Dept. of Education) Sections 73, 74	The Trust/schools do not have to keep copies of DBS certificates. If the Trust/school do so the copy must NOT be retained for more than 6 months	Secure disposal
5.5	Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Yes		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file	Secure disposal
5.6	Pre-employment vetting information – evidence proving the right to work in the United	Yes	An employer's guide to right to work checks [Home Office May 2015]	Where possible these documents should be added to the Staff	Secure disposal

	Kingdom			Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years	
5.7	Staff personal file – staff NOT working with children	Yes	Limitation Act 1980 (Section 2)	Termination of Employment + 6 years	Secure disposal
5.8	Staff personal file – staff working with children	Yes		Termination of employment + 25 years	Secure disposal
5.9	Timesheets	Yes		Current year + 6 years	Secure disposal
5.10	Annual appraisal/ assessment records	Yes		Current year + 5 years	Secure disposal

6.	**Personnel records**				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
6.1	Timesheets, sick pay	Yes		Current Year + 6 years	Secure disposal
6.2	Staff personal files	Yes	Limitation Act 1980 (Section 2)	Termination + 6 years	Secure disposal
6.3	Interview notes and recruitment records	Yes		Date of interview + 6 months	Secure disposal
6.4	Pre-employment vetting information (including CRB/DBS checks)	No	CRB / DBS guidelines	Date of check + 6 months	Secure disposal
6.5	Disciplinary proceedings	Yes	Warnings will not be referred to outside the parameters of the scope	Where the warning relates to child protection issues	Secure disposal

6.	Personnel records				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
				contact LADO for further advice. Otherwise termination + 6 years.	
6.6	Records relating to accident / injury at work	Yes		Date of incident + 12 years. In the case of serious incident further retention period will need to be applied	Secure disposal
6.7	Annual appraisal/assessment records	No		Current year + 5 years	Secure disposal
6.8	Pay slips	Yes		Last date of employment + 85 years	Secure disposal
6.9	Maternity / paternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)	Current year + 3 years	Secure disposal
6.10	Records held under retirement benefits schemes (information powers) regulations 1995	Yes		Current year + 6 years	Secure disposal

7.	Health & safety				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
7.1	Accessibility plans		Disability Discrimination Act	Current year + 6 years	Secure disposal
7.2	Accident reporting		Social Security (Claims & Payments) Regulations 1979		Secure disposal

7.	Health & safety				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
	Adults Children	Yes Yes	Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980	Date of incident +7years DOB of child + 25 years	
7.3	Record of Medicinal Product Administered on the premises, including the date and circumstances of its administration, by whom it was administered, including medicinal products which the child is permitted to administer alone, together with a record of parents' consent.	Yes		DOB of child + 25 years	Secure disposal
7.4	Medical records as specified by the control of substances hazardous to health which also includes health surveillance (e.g. hearing tests, vibration white finger)			Current year + 40 years (where appropriate an additional retention period may be allocated)	Secure disposal
7.4	Incident reports	Yes		Current year + 20 years	Secure disposal
7.5	Policy statements	No		Date of expiry + 1 year	Secure disposal
7.6	Risk assessments	Yes		Current year + 3 years	Secure disposal
7.7	Process of monitoring areas where employees and persons are likely to have become in contact with asbestos (including asbestos plans)	No	Control of asbestos at work regulations	Last action + 40 years	Secure disposal

7.	Health & safety				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
7.8	Process of monitoring areas where employees and persons are likely to have become in contact with radiation	No	Ionising radiations regulations 1999	Last action + 50 Years (or until the person reaches 75 years of age	Secure disposal
7.9	Fire precautions log books (including evacuation logs)	No		Current year + 6 years	Secure disposal
7.10	Emergency lighting testing and log books	No		Current year + 6 years	Secure disposal
7.11	Gas safety certificates	No		Current year + 6 years	Secure disposal
7.12	Fixed electrical testing	No		Current year + 6 years	Secure disposal
7.13	Portable appliance testing	No		Current year + 6 years	Secure disposal
7.14	Legionella testing and log books	No		Current year + 6 years	Secure disposal

8.	Pupil's/student's educational record				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
8.1	Pupil's educational record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437		
8.2	Primary	Yes		Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. This will include:

8.	Pupil's/student's educational record				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
					• to another primary school • to a secondary school • to a pupil referral unit • If the pupil dies whilst at primary school the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period. Primary schools do not ordinarily have sufficient storage space to store records for pupils who have not transferred in the

8.	Pupil's/student's educational record				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
					normal way. It makes more sense to transfer the record to the Local Authority as it is more likely that the pupil will request the record from the Local Authority
8.3	Secondary	Yes	Limitation Act 1980 (Section 2)	Date of birth of the pupil + 25 years	Secure disposal
8.4	Examination results – pupil copies	Yes			
8.4.1	Public			This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.
8.4.2	Internal			This information should be added to the pupil file	

9.	Child protection files				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
9.1	Child protection information held on pupil files	Yes	"Keeping children safe in education statutory guidance for schools and colleges March 2015".	DOB + 25 Years * *It is recommended that all records relating to child*	Secure disposal

			"Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	*abuse are retained until the National Child Abuse Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention*	
9.2	Child protection information held in separate files	Yes	Employment Practices Code: Supplementary Guidance 2.13.1 (records of Disciplinary and Grievance) Education Act 2002 guidance "Dealing with Allegations of Abuse against Teachers and Other Staff" November 2005	DOB of the child + 25 years then review This retention period is on the understanding that the principal copy of this information will be found on the Local Authority records	Secure disposal

10.	**Attendance**				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
10.1	Attendance registers	Yes	School attendance: departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.	Secure disposal
10.2	Correspondence relating to authorised absence	Yes	Education Act 1996 Section 7	Current academic year + 2 years	Secure disposal

11.	Special educational needs				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
11.1	Special educational needs files, reviews, and individual education plans	Yes	Limitation Act 1980 (Section 2)	Date of birth of the pupil + 25 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. An SEN file may be kept for a longer period of time for defense in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented.
11.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	Secure disposal unless the document is subject to a legal hold
11.3	Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	Secure disposal unless the document is subject to a legal hold
11.4	Accessibility strategy	Yes	Special Educational Needs and Disability	Date of birth of the pupil + 25 years [This would	Secure disposal

11.	Special educational needs				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
			Act 2001 Section 14	normally be retained on the pupil file]	unless the document is subject to a legal hold

12.	Curriculum				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
12.1	Curriculum returns	No		Current Year + 3 Year	Secure disposal
12.2	Examination results (schools' copy)	Yes		Current Year + 6 Year	Secure disposal
12.2.1	SATS records –	Yes			Secure disposal
12.2.2	Results			The SATS results should be recorded on the pupil's educational file and will therefore, be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison	Secure disposal

12.	Curriculum				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
12.2.3	Examination papers			The examination papers should be kept until any appeals/validation process is complete	Secure disposal
12.3	Published admission number (PAN) reports	Yes		Current year + 6 years	Secure disposal
12.4	Value added and contextual data	Yes		Current year + 6 years	Secure disposal
12.5	Self-evaluation forms	Yes		Current year + 6 years	Secure disposal

13.	Implementation of curriculum				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
13.1	Schemes of work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL
13.2	Timetable	No		Current year + 1 year	
13.3	Class record books	No		Current year + 1 year	
13.4	Mark books	No		Current year + 1 year	
13.5	Record of homework set	No		Current year + 1 year	
13.6	Pupils' work	No		Where possible pupils' work should be returned	Secure disposal

13.	Implementation of curriculum				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
				to the pupil at the end of the academic year if this is not the school's policy then current year + 1 year	

14.	Educational visits outside the classroom				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
14.1	Records created by schools to obtain approval to run an educational visit outside the classroom – primary schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice	Date of visit + 14 years	Secure disposal
14.2	Records created by schools to obtain approval to run an educational visit outside the classroom – secondary schools	No	Outdoor education advisers' panel national guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice	Date of visit + 10 years	Secure disposal
14.3	Parental consent forms for school trips where there has been no major incident	Yes		Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and

14.	Educational visits outside the classroom				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
					most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time.
14.4	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	Secure disposal

15.	Walking bus				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
15.1	Walking bus registers	Yes		The date of the register + 3 years This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report	Secure disposal [if these records are retained electronically, any back-up copies should be destroyed at the same time]

15.	Walking bus				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
				and kept for the period of time required for accident reporting	

16.	Family liaison officers and home school liaison assistants				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
16.1	Day books	Yes		Current year + 2 years then review	Secure disposal
16.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		Whilst child is attending school and then destroy	Secure disposal
16.3	Referral forms	Yes		While the referral is current	Secure disposal
16.4	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	Secure disposal
16.5	Contact database entries	Yes		Current year then review, if contact is no longer active then destroy	Secure disposal
16.6	Group Registers	Yes		Current year + 2 years	Secure disposal

17.	Local authority and central government liaison				
	Basic file description	**Data protection issues**	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
17.1	Secondary transfer sheets (primary)	Yes		Current year + 2 years	Secure disposal
17.2	Attendance returns	Yes		Current year + 1 year	Secure disposal
17.3	School census returns	No		Current year + 5 years	Secure disposal
17.4	OFSTED reports and papers	No		Life of the report then REVIEW	Secure disposal
17.5	Returns made to central government	No		Current year + 6 years	Secure disposal

Appendix G: Surveillance checklist

School name:	

Name and description of surveillance system:		
The purpose and requirements of the system are address by the system (i.e. the cameras record the required information).	**Yes**	**No**
	Notes:	
The system is still fit for purpose and produces clear images of adequate resolution.	**Yes**	**No**
	Notes:	
Cameras are sited in effective positions to fulfil their task.	**Yes**	**No**
	Notes:	
Cameras are position so that they avoid capturing the images of persons not visiting the premises and/or neighbouring properties.	**Yes**	**No**
	Notes:	
There are visible signs showing that CCTV is in operation. These signs include: • who operates the CCTV • their contact details • what the purpose of the CCTV is.	**Yes**	**No**
	Notes:	
CCTV recording are securely stored and access limited	**Yes**	**No**
	Notes:	
The system has the capability to transfer recordings to law enforcement or to fulfil a request for an individual's own personal information.	**Yes**	**No**
	Notes:	

The system has a set retention period. This retention period should only be long enough to fulfil the CCTV's purpose and not longer. Outside of this retention period, information should be deleted.	**Yes**	**No**
	Notes:	
The system users should be able to selectively delete information still inside the retention period to fulfil the right to erasure.	**Yes**	**No**
	Notes:	
All operations have been authorised by the information asset owner and have sat their mandatory data protection training.	**Yes**	**No**
	Notes:	
This system has been declared on the corporate register of surveillance systems.	**Yes**	**No**
	Notes:	

Checklist completed by:	
Name:	
Job title:	
Date:	

Checklist reviewed and signed by (information asset owner):	
Name:	
Job title:	
Date:	