GDPR POLICY 2018 – 2020

General Data Protection Regulation (2018)
Privacy Notice - Data Protection Act (1998)

Contents

1. Scope

This policy is designed to recognise and address the school's responsibilities pertaining to the Data Protection Act (1998) as well as the General Data Protection Regulations Act (2018), and to lay out how the school will handle, process, secure and then destroy personal and 'sensitive' personal data relating to all stakeholders in the school.

In the discharge of its duties and to comply with statutory and moral obligations , Hetton School will collect and retain and share information from many sources including parents, carers, students themselves, the Local Authority, Social Services, the Police, suppliers, external contractors and agencies. All of this information will be retained by the school for varying amounts of time in order to comply with statutory and other rules of retention.

We hold personal data pertaining to students and their families in order to:

- Support teaching and learning;
- Monitor and report on progress;
- Provide appropriate pastoral care, and
- Assess how well this school is doing.

2. Principles of GDPR

By the terms of GDPR legislation, Hetton School recognises its obligations as stated below from Article 5 of the GDPR that personal data shall be:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date;

e) 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; and

f) processed in a manner that ensures appropriate security of the personal data."

3. Data Controller / Processor recognition

Under the terms of GDPR **Hetton School is the Data Controller**, meaning we are the people who collect and control the data relating to things that happen in the school and for those whose data we personally collect. Article 5 (2) of the GDPR states that *"the controller shall be responsible for, and be able to demonstrate, compliance with the principles [of GDPR]."* We document all the applicable information under Article 30(1) of the GDPR.

Organisations and individuals who access, collate, use and report on that data in their lawful and legitimate dealings with the school are known as **Data Processors**.

These Data Processors can include :

- Teachers
- Administration, pastoral and ancillary staff
- The Local Authority (for Payroll & HR, School Finance, Together For Children, Governance support, SEND provision)
- SIMS (our school management information system)

- SAP (our finance system)
- CAMHS
- Attendance 100
- CRB Cunninghams (catering services provision)
- Local colleges and universities
- Contractors, service provision companies and telephony
- CCTV provision

This list is not exhaustive.

As Data Processors we document (or ensure that all processors of the data document) all the applicable information under Article 30(2) of the GDPR.

4. Roles and responsibilities

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

Governing board

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

Data Protection Officer

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

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

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

Our DPO is Gateshead Council. Tanya Rossington is contactable on 0191 433 2192.

Headteacher

The Headteacher acts as the representative of the Data Controller on a day-to-day basis.

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure

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

5. Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- 'Pseudonym-isation' to ensure protection where possible
- Create and improve security features on an ongoing basis
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
  - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

Whilst preparing to document our processing activities we:

- conducted information audits to find out what personal data our organisation holds;
- talked to staff across the organisation to get a more complete picture of our processing activities; and
- reviewed our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

As part of our record of processing activities we document, or link to documentation, on:

- information required for privacy notices;
- records of consent;
- controller-processor contracts;

- the location of personal data;
- Data Protection Impact Assessment reports; and
- records of personal data breaches.

We document our processing activities in electronic form so we can add, remove and amend information easily.

Personal data that we may collect, use, store and share (when appropriate) **about students** includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data

We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing

If students are enrolled for post-14 (KeyStage 4) qualifications we will be provided with their unique learner number (ULN) by the Learning Records Service and may also obtain from them details of any learning or

qualifications that has been undertaken. The same will be true from the primary school that students join us from.

We process data relating to **those we employ**, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and / or grievance procedures
- Absence data
- Copy of driving licence
- Photographs
- CCTV footage
- Data about your use of the school's information and communications system

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

Why we use this data

The purpose of processing this data is to help us run the school, including to:

- Enable staff to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards students
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

6. Legal Bases

We will hold this information according to one of the six legal bases for holding personal data. They are

- **Legal obligation**, where the school is legally required to retain this information (eg under Education Act 2011), and this basis overrides all others
- **Public task** such as fulfilment of our role in facilitating the education of children, but only where it is 'necessary', and overrides any requirement for consent

- **Vital interests**, such as life-or-death health-related matters where consent is not required, and has not been withdrawn
- **Consent**, where consent is explicitly requested as an opt-in (not opt-out), and can be withdrawn at any time
- **Contractual requirement**, where data is held to fulfil the terms of a contract between the school and the person whose data it is
- **Legitimate interest**, where we would use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing. To use this reason the school would identify the legitimate reason, and justify that it would not outweigh the rights or privacy of the individual.

The different types of data that is held by us is detailed in our Data Map – Appendix B.

Consent

Where the legal basis for holding personal data is 'Consent', it will always be the case that, on the form where consent is requested, that each individual amount of data is stipulated, and consent is sought on a granular level.

The GDPR guidelines are that consent should be sought only if it will be:

- *freely given* – consent must not be conditional on a service;
- *specific* – one consent for one issue, should not lump issues together;
- *informed* – the data subject should be informed on its use – how it will be used, by whom and how they can withdraw their consent;
- *unambiguous* – must be simple to understand and specific;
- *clear affirmative action* – an individual must agree in some tangible way that a data controller can record and keep their personal data so that the data controller can prove it was given and what they were told, when and how the data subject gave their consent

It will also be the case that the data subject will be informed of their right to withdraw this consent at any time.

The school will take reasonable steps to ensure that, where consent is requested and given digitally, that the consent is being given by the person required to give consent, and not a third party. These steps may include a phone call to verify that consent was in fact given, or a hard copy is sent back at a later time with a physical signature where a more speedy (digital) response is needed in the interim.

7. Right to deletion

Under the terms of GDPR it is the case that any person whose data is held for reasons other than a legal basis have the right to have their data deleted (the right to be forgotten) or transferred to another party, notwithstanding any data of a commercial nature or that which would compromise the privacy rights of others.

8. Right of access

Subject access requests

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

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

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

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

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

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond within 30 days of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 30 days, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests

- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

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

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

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

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

9. Data Sharing

School has an Information Sharing Protocol (policy) and a Freedom of Information Policy, both of which should be read in conjunction with this section.

The school may *receive* information from 'feeder' Primary schools and the Learning Records Service (among others) about students and their education / pastoral needs to assist in the discharge of our public duty of

education. This information will form a part of each student's file, and as such we will assume the data controller responsibilities for this information.

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

- There is an issue with a pupil or parent / carer that puts the safety of our staff at risk. This forms part of our statutory duty and is referred to further in the retention map (Appendix B).
- We are also required by law to pass information about students to the Local Authority and the Department for Education (DfE); to another school or setting where the child will transfer to, or to further / higher education establishments.
- We need to liaise with other agencies (we will seek consent where necessary before doing this)
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils (for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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

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

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

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Once students are aged 13 or over, we are required by law to pass on certain information to the provider of youth support services in their area. This is the local authority support service for young people aged 13 to 19 in England. We must provide the student's address (usually that of their parent(s) / guardian), plus the student's date of birth and any further information relevant to the support services' role.

However, until the student is aged 16 or older, their parent(s) / guardian can ask that no information beyond the name, address and date of birth (and *their* name and address) be passed on to the youth services provider. This right transfers to the student on their 16th birthday.

For more information about young peoples' services, please go to the Directgov Young People page at https://www.gov.uk/topic/schools-colleges-childrens-services/support-for-children-young-people

The Police and other agencies may request data to be shared with them. The school reserves the right under its obligations as the Data Controller to balance the privacy of the subject and any other stakeholders against the likelihood of harm if the data is withheld.

Contracts are maintained between Hetton School and all Data Processors who use the data collated by the school. The contents of the contracts are consistent with the demands of GDPR and ensure that all groups and

persons utilising this data in any way respect and protect the privacy of their systems and processes at all times, and that the data is deleted effectively when either the contract ends, or when the use of that data has passed. See below.

Further to the above, individuals have the right to request that data is ported to another controller without any detriment to its usability.

10. Usage contracts

Staff are required to sign the Acceptable Use policy, which is detailed in appendix A. This is Hetton school's policy for staff to act responsibly when dealing with student information. It also sets out standards for ensuring encryption of data when at school, but also when away from school.

Contracts are required for the following Data Processors who have been identified as at Feb 2018 as having access to school personal and sensitive personal data :

- Local Authority
- SIMS
- Health & Safety Executive
- The Police
- DFE
- Various exam boards
- NHS
- Derwent Hill (Evolve system)
- Social Services
- CAMHS
- CPOMS
- Schools Letting Solutions
- SAP
- Attendance 100
- CRB Cunninghams
- Konica Minolta
- University of Newcastle upon Tyne
- Sunderland College

11. Profiling

Hetton School does not carry out automated decision-making and profiling of data. This does not affect the individual's rights to have access to all data held on them.

12. Retention

Hetton School recognises that by efficiently managing its records it will be better able to comply with its legal and regulatory obligations, and to contribute to the effective overall management of the school. Records provide evidence for protecting the legal rights and interests of the school and its stakeholders, and provide evidence for demonstrating performance and accountability.

Hetton School will retain documents and records in line with the data mapping schedule appended to this document. The guidelines contained therein are based upon the Information and Records Management Society (IRMS) Information Management Toolkit for Schools v5 (01 Feb 2016). This applies to all records created, received or maintained by staff of the school in the course of carrying out its functions, retained for a set period to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically, as detailed in the appended schedule. (Appendix B)

Student record retention

Hetton School believes that student files and records should be retained unadulterated in the state that they are originally archived after the student leaves. Therefore Hetton School will not purge individual documents and pieces of paper from a student record due to the risk of :

a) accidentally removing and destroying a piece of information which may subsequently become important
b) rules of retention for an item extending in future, meaning that a previously removed document should at some point have been retained according to the new guideline

Retention guidance in school

The person responsible for records management in the school 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.

Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the school's records management guidelines (Appendix B).

13. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

14. Further information

If individuals require more information about how the Local Authority (LA) and/or DfE store and use their information, then please go to the following websites:

https://www.sunderland.gov.uk/information-charter

http://media.education.gov.uk/assets/files/doc/w/what%20the%20department%20does%20with%20data%20on%20pupils%20and%20children.doc

If these websites cannot be accessed we can send copies of this information.

Please write to The Information Manager
Governance Services

Civic Centre
SUNDERLAND SR2 7DN

Alternatively contact the Ministerial and Public Communications Division
Department for Education
Piccadilly Gate
Store Street
MANCHESTER M1 2WD
Website: https://www.gov.uk/contact-dfe
Telephone: 0370 000 2288

Or contact Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Website https://ico.org.uk/
Telephone: 0303 123 1113 (local rate) or 01625 545 745 (national rate)

Appendix A

ICT Acceptable Use Agreement: Staff, Governors and Visitors

- As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff and Governors are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy. Visitors (such as supply staff and others working with students and/or those who have access to school ICT systems are also asked to read and sign.

- This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, smart watches, digital cameras, email and social media sites.

2. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

4. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly.

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the network manager.

6. I will ensure that any personal data of students, staff or parents/carers is kept in accordance with the Data Protection Act 1998. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely. Any such data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of students will only be used as stated in the school image use policy and will always take into account parental consent.

7. I will not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted (password/passcode protected). Where possible I will use the Virtual Learning Environment, the approved remote access or the school level of Sunderland's Office 365 to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.

8. I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

9. I will respect copyright and intellectual property rights.

10. I have read and understood the school ICT Use policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of students within the classroom and other working spaces (please also refer to the letter on Social Media from the Headteacher).

11. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead (Jane McKeown) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Headteacher (Craig Knowles) and/or Designated Safeguarding Lead (Jane McKeown) as soon as possible.

12. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the ICT Support Provider/Team/lead (Keith Woods) as soon as possible.

13. My electronic communications with students, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher.

14. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.

15. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the Local Authority, into disrepute.

16. I will promote online safety with the students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

17. I understand that I am still in a position of power with ex-students and therefore should not engage with them through social media or any other channels not prior approved by the Designated Safeguarding Lead (Jane McKeown).

18. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead (Jane McKeown) and/or the Head Teacher (Craig Knowles).

19. Where there are specific uses of technology within school (e.g. tablets, voting pads etc.) this should be done so in line with school policies and the law. All reasonable steps must be taken to ensure mobile devices remain secure.

20. I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

Adopted January 2018

What data do we have?	Data can include	Consent required?	Legal basis for retention	Storage method	Old guidelines of retention period	Method of disposal	Where is it kept?	How long do WE keep it	Who accesses this data internally?	Who processes this data externally?	Are processors GDPR-contracted?
STAFF											
Staff files - current	Name, address, next of kin, bank details, health details, CV, references, DBS, DFE #, qualifications, appraisals, leave of absence, disciplinary info, pension, application form	No	Legal obligation	Paper & SCR	Termination + 6 yrs	Secure disposal	HT office	Termination + 6 yrs	H/T, H/T PA & SBM	LA / SIMS	No
Staff files - archived	Name, address, next of kin, bank details, health details, CV, references, DBS, DFE #, qualifications, appraisals, leave of absence, disciplinary info, pension, application form	No	Legal obligation	Paper	Termination + 6 yrs	Secure disposal	Archive room	Termination + 6 yrs	H/T, H/T PA & SBM	LA / SIMS	No
Interview notes & recruitment records	Notes taken at interview	No	Legal obligation	Paper	Interview + 6 months	Secure disposal	HT / Archive room	Interview + 6 months	H/T, H/T PA & SBM	N/A	No
Pre-employment vetting info	Three forms of ID	No	Legal obligation	Paper & SCR	Date + 6 months	Secure disposal	HT / Archive room	School keep ID for	H/T, H/T PA & SBM	N/A	No

								teachers on file			
Accident at work records (staff)	Medical information	No	Legal obligation	Paper & digital	Incident + 12 yrs	Secure disposal	Archive room / LA	Incident + 12 yrs, and since 2016 kept digitally by SCC	Admin	LA	No
Asbestos incidents	Medical information	No	Legal obligation	Paper	Date + 40 years	Secure disposal	LA	Date + 40 years	Admin	LA / HSE	No
Appraisal records	Appraisal meeting notes & outcomes	No	Legal obligation	Paper	Date + 5 yrs	Secure disposal	HT office & Line Managers	Kept on file	H/T, H/T PA, SBM & managers	N/A	No
Salary records	Pay levels, increases, TLR payments	No	Legal obligation	Digital	Terminatio n + 85 yrs	Secure disposal	SBM office (digital)	Termination + 85 yrs	H/T, H/T PA & SBM	LA	No
Allegations of CP nature against staff	Interview notes, meeting notes & outcomes	No	Legal obligation	Paper & digital	No less than 10yrs, then until retirement	Secure disposal	HT office	No less than 10yrs, then until retirement	H/T, S/L	LA / Police	No
Staff Timesheets (incl absence)	Reasons for absence / overtime	No	Legal obligation	Paper	Date + 6 years	Secure disposal	SBM office (hard copy)	Date + 6 years	Admin	LA	No
STUDENT											
Accident reporting (student)	Name, address, date of birth, medical info	No	Legal obligation	Paper & digital	DOB + 25 years	Secure disposal	Archive room / LA	Incident + 12 yrs, and since 2016 kept digitally by SCC	Admin	LA / SIMS	No
Student folders - current	All student data. Name, address, contact details, medical info	No	Legal obligation	Paper	DOB + 25 years	Secure disposal	Head-of-year office	DOB + 25 years	Teachers / Admin	N/A	No

Student folders - archived	All student data. Name, address, contact details, medical info	No	Legal obligation	Paper	DOB + 25 years	Secure disposal	Archive room	DOB + 25 years	Teachers / Admin	N/A	No
Examination results - school's copy	Name, age, results	No	Legal obligation	Paper & digital	DOB + 6 years	Secure disposal	Exams office	DOB + 6 years	Teachers / Admin	DfE L/A	No
Examination results - pupil's copy	Name, age, results	No	Legal obligation	Paper	1 Year	Secure disposal	Exams office within Secure Storeage	1 Year	Exams Officer/SBM	Exam board / DfE	No
SEN statement/EHCP	Name, age, contact info, medical information, meeting reports, parental information	No	Legal obligation	Paper & digital	DOB + 25 years	Secure disposal	Archive room	DOB + 35 years	SENCO / Admin	LA / NHS	No
Advice to parents on SEN	Name, age, contact info, medical information, meeting reports, parental information	No	Legal obligation	Paper & digital	DOB + 25 years	Secure disposal	Archive room	DOB + 35 years	SENCO / Admin	LA / NHS	No
SEN files & IEP's - current	Name, age, contact info, medical information, meeting reports, parental information	No	Legal obligation	Paper & digital	DOB + 25 years	Secure disposal	Archive room	DOB + 35 years	Teachers / Admin	LA / NHS	No
SEN info - archived	Name, age, contact info, medical information, meeting reports, parental information	No	Legal obligation	Paper & digital	DOB + 25 years	Secure disposal	Archive room	DOB + 35 years	SENCO / Admin	LA / NHS	No
Parental permission - no incident	Name	Yes	Consent	Paper	End of visit	Secure disposal	Archive room	End of visit	Teachers / Admin	N/A	No

Parental permission - major incident	Name, age, contact info, medical information, meeting reports, parental information	No	Legal obligation	Paper	DOB + 25 years	Secure disposal	Archive room	DOB + 25 years	Teachers / Admin	LA / HSE	No
EVC records of trips	No sensitive data	No	Legal obligation	Digital	Date + 10 yrs	Secure disposal	Kept online by Evolve system	Kept online by Evolve system	Teachers / Admin	Evolve	No
Free school meal registers	Name, age, address, parental information	No	Legal obligation	Digital	Current year + 6 yrs	Secure disposal	Archive room	Current year + 6 yrs	Teachers / Admin	LA	No
Child protection files held in student file	Name, age, contact info, medical information, meeting reports, parental information	No	Legal obligation	Paper	DOB + 25 years (in sealed envelope)	Secure disposal	Archive room	DOB + 25 years (in sealed envelope)	H/T, S/L	LA / SServs / CAMHS / Police	No
Child protection files held in separate file	Name, age, contact info, medical information, meeting reports, parental information	No	Legal obligation	Paper	DOB + 25 years (main copy to be with LA)	Secure disposal	Archive room	DOB + 25 years (main copy to be with LA)	H/T, S/L	LA / SServs / CAMHS / Police	No
ADMIN / PREMISES / FINANCE											
Visitors book	Name, company worked for	No	Legitimate interest	Paper	Date + 6 years	Review and document if further retention required	Archive room	Date + 6 years	Admin	N/A	No
School lettings info	Name, address, contact info	No	Legitimate interest	Paper & digital	Current Fin. Yr + 6yrs	Secure disposal	Archive room	Current Fin. Yr + 6yrs	Admin	SLS	No
Contractual info	Name, address, contact info, potential financial info (not sensitive)	No	Legal obligation	Paper & digital	Last payment + 6 years	Secure disposal	SBM office / Archive	Last payment + 6 years	Admin	Various	No

							room / server				
Financial data - current	Names, payment details, contact info	No	Legal obligation	Digital	Current year + 6 yrs	Secure disposal	SAP	Current year + 6 yrs	Teachers / Admin	LA / SAP	No
Financial data - archived	Names, payment details, contact info	No	Legal obligation	Paper & digital	Current year + 6 yrs	Secure disposal	SAP / Archive room	Current year + 6 yrs	Admin	LA / SAP	No
Admissions info, incl proof of address	Name, age, contact info, medical information, meeting reports, parental information	No	Legal obligation	Paper	Admission + 1 yr	Secure disposal	Head of Year office	Admission + 1 yr	Teachers / Admin	LA	No
Admission register	Name, age, contact info, medical information, meeting reports, parental information	No	Legal obligation	Digital	Final date + 6 yrs??	Secure disposal	SIMS	Final date + 6 yrs??	Teachers / Admin	LA	No
Attendance register	Name, age, address	No	Legal obligation	Digital	Date + 3 yrs	Secure disposal	SIMS	Date + 3 yrs	Teachers / Admin	LA / Att100 / SServs	No
Authorised absence info	Name, age, address, parental information	No	Legal obligation	Paper & digital	Current year + 2 yrs	Secure disposal	Head of Year office / Archive room / SIMS	Current year + 2 yrs	Teachers / Admin	LA / Att100 / SServs	No
Markbooks, Homework records, Pupil work	Name, age	No	Legitimate interest	Paper & digital	Date + 1 yr	Secure disposal	Head of Year office	Date + 1 yr	Teachers / Admin	N/A	No

PROGRAMMES IN SCHOOL											
Attendance 100	Name, age, address, parental information	No	Contractual requirement	Paper & digital	Date + 3 yrs	Secure disposal at end of contract	L.Kell office	Date + 3 yrs	Teachers / Admin	Att100	No
SIMS	Name, age, contact info, medical information, meeting reports, parental information, student performance, behaviour	No	Legal obligation	Digital	DOB + 25 years	Secure disposal	LA / server	DOB + 25 years	Teachers / Admin	SIMS	No
SAP	Names, payment details, contact info	No	Legal obligation	Digital	Current year + 6 yrs	Secure disposal	LA / server	Current year + 6 yrs	Admin	SAP	No
CPOMS	Name, age, contact info, medical information, meeting reports, parental information, student performance, behaviour	No	Legal obligation	Digital	DOB + 25 years	Secure disposal	Internal server	DOB + 25 years	Teachers / Admin	N/A	No
Tassomai	Name, age (?)	Yes	Public task	Digital	DOB + 25 years	Secure disposal at end of contract	Online	DOB + 25 years	Teachers / Admin	Tassomai	No
CRB Cunninghams	Name, biometric equivalent data, financial & dietary records	Yes	Contractual requirement	Digital	Current Fin. Yr + 6yrs	Secure disposal at end of contract	Internal server	Current Fin. Yr + 6yrs	Teachers / Admin	CRB Cunninghams	No
Konica Minolta	Copies of documents processed. Could be any information	No	Contractual requirement	Digital	End of contract	Secure disposal at end of contract	Internal server	End of contract	Admin	Konica Minolta	No

POTENTIAL NON-DATA BREACHES											
Items taken from desks	Could be any information	N/A	N/A	Paper & digital	N/A	N/A	In office / classroom	N/A	N/A	N/A	N/A
Keys lost	Potential fo any information taken	N/A	N/A	Paper & digital	N/A	N/A	In office / classroom	N/A	N/A	N/A	N/A
POTENTIAL BREACHES OUTSIDE SCHOOL											
Memory sticks taken from school	Could be any information	N/A	N/A	Digital	N/A	N/A	Outside school	N/A	N/A	N/A	N/A
Remote log-in / printing / memory sticks	Could be any information	N/A	N/A	Paper & digital	N/A	N/A	Outside school	N/A	N/A	N/A	N/A
Future Me project data	Small number of cases not anonymised	Yes	Legitimate interest	Digital	End of contract	Secure disposal at end of contract	Outside school	End of contract	N/A	Newcastle Uni / Glass box	Yes