Saint Nathaniel's Academy
E-Safety Policy

E-Safety Policy

Scope of the Policy

This policy applies to all members of the *academy* community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of academy ICT systems, both in and out of the *academy*.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *academy* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school / academy, but is linked to membership of the academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The *academy* will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

What is E-Safety?

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

End to End E-Safety

E-Safety depends on effective practice at a number of levels:

Responsible ICT use by all staff and pupils in school and at home; encouraged by education and made explicit through published policies.

Sound implementation of E-Safety policy in both administration and curriculum, including secure school network design and use.

Safe and secure broadband including the effective management of filtering.

Reviewing the E-Safety policy

The E-Safety Policy relates to other policies including those for ICT, bullying, RSE and for child protection (safeguarding). The ICT curriculum coordinator will also act as E-Safety coordinator. The E-Safety Policy and its implementation will be reviewed regularly.

Teaching and learning - why Internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning.

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access
School ICT systems capacity and security will be reviewed regularly.
Virus protection will be updated regularly.
Security strategies will be discussed within Saint Bart's Trust.

E-mail
(Currently blocked and only opened if Teacher requests e.g. covering within the curriculum)
Pupils may only use approved e-mail accounts/messaging systems on the school system.
Pupils must immediately tell a teacher if they receive offensive e-mail or messages.
Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Published content and the school learning platform
The contact details on the Web site must be the school address, e-mail and telephone number.
Staff or pupils' personal information will not be published.

Publishing pupils' images and work
Photographs that include pupils will be selected carefully. Only pupils who have written parental permission will be displayed on the website.
Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
Written permission from parents or carers will be obtained before photographs of pupils or pupils' work are published on the school Web site. This is done on entry to school.
No photographs of Looked after Children should be displayed.

Social networking and personal publishing
The school will block/filter access to social networking sites.
Newsgroups will be blocked unless a specific use is approved.
Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Managing filtering
The school will work with the LA, Stoke on Trent Safeguarding board and the Internet Service Provider (school's broadband) to ensure systems to protect pupils are reviewed and improved.
If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Coordinator. (Mr Field who will directly report to SLT and the ICT technicians who will block the site).
The ICT co-ordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions (ICT co-ordinator to give a copy of the policies to all members of staff)
Authorising Internet access
All staff must read and adhere to the acceptable use policy before using any school ICT resource.
Access to the Internet will be by supervised access to specific, approved on-line materials.
All staff must read and understand the related computing policies (see Related policies).

Assessing risks
The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor local authority can accept liability for the material accessed, or any consequences of Internet access. If unsuitable material appears, the E-Safety coordinator & SLT will be informed so that relevant filtering can be completed.
The school will audit ICT provision to establish if the E-Safety policy is adequate and that its implementation is effective.

Handling E-Safety complaints
Complaints of Internet misuse will be dealt with by the class teacher and where necessary a senior member of staff. Teachers to log the incident on CPOMS under E-Safety.
Any complaint about staff misuse must be referred to the Head teacher.
Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Community use of the Internet
External organisations using the school's ICT facilities must adhere to the E-Safety policy.
Internet use by staff and children is actively monitored.

Communicating the E-Safety Policy
E-Safety SMART rules will be posted in all networked rooms and discussed with the pupils at the start of each year and throughout the year as part of computing and PHSE sessions.
Pupils will be informed that network and Internet use will be monitored.

Staff and the E-Safety policy
All staff will be given the School E-Safety Policy and its importance explained.
Staff should be aware that Internet traffic can be monitored and traced to the individual user.
Discretion and professional conduct is essential.

Enlisting parents' support
Parents' attention will be drawn to the School E-Safety Policy in newsletters and the school prospectus. Any e-safety concerns will be shared with parents via tweets, and newsletters.
The school website provides information to help parents.

Prevent: Radicalisation and Extremism
Saint Nathanial's Academy takes an active role in protecting pupils from the risks of extremism and radicalisation. Keeping children safe from risks posed by terrorist exploitation of social media is approached in the same way as safeguarding children from any other online abuse. In the same way teachers are vigilant about signs of possible physical or emotional abuse, we are vigilant about any signs of radicalisation or extremism in any of our pupils. We follow the same safeguarding procedure to ensure all children in our care are well looked after.
For more information on Prevent, Radicalisation and Extremism please follow the link on our website on the E-Safety page.

Related policies
There are a number of other policies at Saint Nathaniel's Academy which relate to the topics mentioned above. It is important that you read and fully understand the polices below which can be found on the Saint Nathaniel's Academy website. If you have any questions about this policy or any other policies please ask Mr Field.

- Staff and volunteer acceptable use policy
- Parents acceptable use policy
- Use of digital and video images
- Pupil acceptable use policy
- St Bart's data protection policy
- Password policy
- Mobile device policy
- Filtering policy
- St Bart's social media policy
- RSE Policy

I have read and understood the e-safety policy and the above policies.

Name _____ Date _____

This policy was reviewed and updated by Mr Field in 2020.
To be reviewed 2021

Staff (and Volunteer) Acceptable Use Policy Agreement School Policy

New technologies have become integral to the lives of children and young people in today's society, both within academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Staff Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the *academy* will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, IPADS, email, virtual learning environments, etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *academy* ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school / academy*:

- When I use my mobile devices (IPADS/ laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school / academy* equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the academy ICT systems.

- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up - See back up procedure.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless I have permission from Mr Field or A. Bath.
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school / academy*:

- I understand that this Acceptable Use Policy applies not only to my work and use of academy ICT equipment in school, but also applies to my use of academy ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the academy
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *students / pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above *pupils*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

Either: (KS2 and above)
I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
Or: (KS1)
I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed | | Date | |

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people can not be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students / pupils* in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree

Digital / Video Images Permission Form

Parent / Carers Name	
Pupil Name	

As the parent / carer of the above *student / pupil*, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.	Yes / No
I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Signed	
Date	

Use of Biometric Systems
The school uses biometric systems for the recognition of individual children for the school canteen.

Biometric technologies have certain advantages over other automatic identification systems as pupils do not need to remember to bring anything with so nothing can be lost, such as a swipe card.

The school has carried out a privacy impact assessment and is confident that the use of such technologies is effective and justified in a school context.

No complete images of fingerprints are stored and the original image cannot be reconstructed from the data. That is, it is not possible for example, to recreate a pupil's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

Parents / carers are asked for permission for these biometric technologies to be used by their child:

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above *pupil*, I agree to the school using biometric recognition systems, as described above. I understand that the images cannot be used to create a whole fingerprint of my child and that these images will not be shared with anyone outside the school.

Yes / No

Signed

Date

Pupil Acceptable Use Policy Agreement– for younger pupils (Foundation / KS1)

This is how we stay safe when we use computers:

I will ask a teacher or suitable adult if I want to use the computers

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computer and other equipment

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Signed (child):……

Signed (parent): ……..

Pupil Acceptable Use Agreement – for KS 2 pupils

Internet Access Rules

For safe use of the Internet at Saint Nathaniel's Academy you will be expected to follow these rules:

1. I will only connect to the Internet during a class lesson when my teacher has told me to do so and only use the web address that my teacher has given me.
2. I may only connect to the Internet during free choice sessions if my teacher has given me permission to do so. I will only access suitable websites.
3. I won't give my username and passwords to anyone else.
4. If I see a message or site that makes me feel uncomfortable I will tell the adult present straight away.
5. At home and school, I will keep information or pictures about myself, my family or my school private. If I am unsure, I will check with an adult.
6. I will be a good on-line citizen and not do anything that hurts other people.
7. I will never agree to meet with someone I have only talked to online.
8. I will not download anything onto the school computers and will check with my parents before downloading anything at home.
9. I understand that the *academy* will monitor my use of the systems, devices and digital communications
10. I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission). I understand that, if I do use my own devices in the school / academy, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

Name of Student / Pupil	
Group / Class	
Signed	
Date	

Data Protection Policy

Contents

Appendix 1: Personal data breach procedure

1. Aims

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

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

2. Policy Scope

This policy applies to:

- All sites within our organisation
- Our teaching staff, support staff, Trustees and Governors
- Contractors, suppliers and anyone working on our behalf

3. Legislation and Guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.
It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.
It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.
In addition, this policy complies with our funding agreement and articles of association.

4. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where

	used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

5. The Data Controller

Each academy processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

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

6. Roles and Responsibilities

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

6.1 Trust Board

The trust board has overall responsibility for ensuring that our academies comply with all relevant data protection obligations.

6.2 Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.
They will provide an annual report of their activities directly to the trust board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.
Full details of the DPO's responsibilities are set out in their job description.
Our DPO is Steve Jones and is contactable via sjones@sbmat.org or 01782 235524

6.3 Principal

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

6.4 All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address

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

7. Data Protection Principles

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

The principles say that personal data must be:

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

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

8. Collecting Personal Data

8.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

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

8.2 Limitation, Minimisation and Accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.
If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.
Staff must only process personal data where it is necessary in order to do their jobs.
When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's retention schedule/records management policy.

9. Sharing Personal Data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep 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.

10. Subject Access Requests and Other Rights of Individuals

10.1 Subject Access Requests

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

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period

- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

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.

10.2 Children and Subject Access Requests

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

10.3 Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

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

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

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

10.4 Other Data Protection Rights of the Individual

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

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

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

11. Parental Requests to see the Educational Record

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

12. Biometric Recognition Systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.
Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.
Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish.
Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.
As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).
Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

13. CCTV

We use CCTV in various locations around the school site to ensure the safety and security of those in our learning community, and to protect the site from damage.. We will adhere to the ICO's code of practice for the use of CCTV.
We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.
Images recorded by the CCTV cameras are stored on a separate server, in a secure location. They are retained for a maximum of **7 / 14 / 21 / 28** days, after which time they are securely overwritten.

Access to the images is restricted to specified people within the school. We will only view CCTV footage in response to an incident or an allegation.
The images on our CCTV system are of a sufficient quality to allow us to make out faces of individuals in most circumstances. We are able to take copies of relevant parts of the CCTV footage and store it securely, in order to assist investigations into incidents or allegations.
In certain circumstances we may share CCTV footage with partners or other agencies. This may include senior leaders, parents, the Local Authority or the Police.
You can ask to see CCTV footage in which your image is captured. This should be done in writing as part of a Subject Access Request.
Any enquiries about the CCTV system should be directed to Jamie Wood via jwood@sbmat.org or 01782 235524

14. Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our school.
We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.
Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.
When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

15. Data Protection by Design and Default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal 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

16. Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our E-Safety Policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

17. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.
For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. Personal Data Breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

19. Training

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

20. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.
This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.

21. Links with other Policies

This data protection policy is linked to our:

- Freedom of Information Publication Scheme
- E-Safety Policy,

Appendix 1:

Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

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

  If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Trust/School computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
    - Records of all breaches will be stored on the Trust/School computer system.
- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

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

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request

that those individuals delete the information and do not share, publish, save or replicate it in any way

- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and delete

Saint Nathaniel's Academy Password Policy

All devices that have access to a) the internet and b) the school network must be password protected. The purpose of this is to prevent data loss and protect pupils and staff.

Staff passwords

Staff each have their own username and unique password. Staff are to come up with their own password and not share it with anybody. Records of staff passwords are not stored but the passwords can be overwritten or reset by the network administrator.

Pupil passwords

Each pupil has their own username and password for software such as purplemash, showbie and TT rockstars. Passwords are generated by teachers and a record of the passwords is stored on the software. Children are taught not to share their passwords with anyone.

USB device password

USB devices are encrypted and password protected. The encryption password is universal.

Hard drive encryption password

Laptop hard drives are encrypted and password protected. The encryption password is universal.

iPad PIN codes

All iPad at Saint Nathaniel's must have a 4 or 6 diget PIN code.

Mobile devices policy

Personal mobile devices - staff

- Staff are not permitted to make/receive calls/texts during contact time with children. Emergency contact should be made via the school office.
- Staff should have their devices on silent or switched off and out of sight (e.g. in a drawer, handbag) during class time.
- Mobile phones should not be used in a space where children are present (e.g. classroom, playground).
- Use of devices (including receiving/sending texts and emails) should be limited to non-contact time when no children are present e.g. in office areas, staff room, empty classrooms.
- Staff are not permitted to take photos or recordings or use any recording software with their personal devices.
- Devices connected to the internet are subject to the same web filtering as any other devices.
- Should there be exceptional circumstances (e.g acutely sick relative), then staff should make the principal and office staff aware of this so messages can be relayed promptly.
- Staff should report any usage of mobile devices that causes them concern to the principal.
- All staff must password protect their mobile device

Personal mobile devices - Visitors

- Visitors are not permitted to make/receive calls/texts during contact time with children. Emergency contact should be made via the school office.
- Visitors should have their devices on silent or switched off and out of sight (e.g. in a drawer, handbag) during class time.
- Mobile phones should not be used in a space where children are present (e.g. classroom, playground).
- Use of devices (including receiving/sending texts and emails) should be limited to non-contact time when no children are present e.g. in office areas, staff room, empty classrooms.
- Visitors are not permitted to take photos or recordings or use any recording software with their personal devices.
- Devices connected to the internet are subject to the same web filtering as any other devices.
- Should there be exceptional circumstances (e.g acutely sick relative), then visitors should make the principal and office staff aware of this so messages can be relayed promptly.
- Visitors should report any usage of mobile devices that causes them concern to the principal.
- All visitors must password protect their mobile device

Personal mobile devices - pupils

- Pupils to only have phones when permission is granted from the school and parents
- Phones to be switched off during the school day

- Emergency Contact to be made through the school office
- Children are not permitted to take photos or recordings or use any recording software with their personal devices.
- Devices connected to the internet are subject to the same web filtering as any other devices.

School owned mobile devices – staff

- All mobile devices including USB sticks must be password protected to prevent data loss
- All mobile devices must be protected by the school's web filtering system
- Passwords to devices must not be shared with anyone who is not employed by the school

School owned mobile devices - pupils

- All mobile devices must be protected by the school's web filtering system
- Devices intended for pupil use must not leave the school
- Pupils must access mobile devices using pupil user accounts only
- Pupil mobile device user accounts must block any attempted file downloads, block access to the computer's system files, block access to the control panel, block access to the command prompt and only map the student network drive.

Miscellaneous

- SSID access code to be held by the IT technician, principal, deputy head and IT Co-ordinator only.

Saint Nathaniel's Academy Internet Filtering Policy

SSID - Jbaskeyfield

All internet use on all devices at Saint Nathaniel's Academy is filtered. The firewall is controlled by the ISP (internet service provider) Talk Straight broadband.

SSID Password
Access to the WIFI is protected by a password. The password is held by the IT Technician and IT co coordinator. The password is not to be given out for any reason.

Connecting a new device
Devices that are not already connected to the network are to be connected by the IT Technician.

Filtering levels
At Saint Nathaniel's Academy there are three levels of web filtering which are controlled and administrated by the IT Technician.

1. Allow all (used by network administrators, SLT and safeguarding staff)
2. Staff web (used by staff not listed above)
3. Pupil web (used by pupils)

Allow all – Free internet use.

Pupil web – Highly restricted web use. Blocks sites and searches based on key words/phrases as well as by category.

Staff web – Works the same as pupil web but with less restrictions allowing staff to search for resources more freely.

Safety net
Filtering levels are assigned to a person based on their username. If a device does not require a username such as a tablet or mobile phone or the username is not recognised by the filtering system, the device is automatically assigned the pupil web filter level.

Globally blocked / globally allowed
We also have the option to add a site to a globally blocked or globally allowed list.

If a member of staff finds a site which they feel should be blocked which isn't, they must report it to the IT Technician who will add it to the globally blocked list.

If a member of staff needs access to a blocked site, they must report it to the IT Technician. The IT Technician is to review the sites content and add it to the globally allowed list if the site is appropriate.

Acknowledgement:

SWGF templates were used to assist the writing of this policy. (http://swgfl.org.uk/products-services/esafety/resources/online-safety-policy-templates)