	Information Security, Online Safety and Data Protection Policy	
	Committee: Students and Staff Committee	
	Co-ordinator : J Day	
	Last Reviewed : Autumn 2023	**Next Review :** Autumn 2025 (or sooner if GDPR legislation changes)
	Policy links to : Privacy Notice	

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for our school to use technology to benefit learners.

Everybody in the school community has a shared responsibility to take reasonable steps to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in information security should be made aware of the risks and threats, and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors - for regulated activities and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc.) and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Principles

Anyone processing personal data must comply with the enforceable principles of good practice.

These provide that personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed; Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to

implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

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

Personal data may only be processed for the specific purposes notified to the Data Subject when the data was first collected, or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the Data Subject must be informed of the new purpose before any processing occurs.

Sensitive Personal Data

The school will be processing sensitive personal data about our stakeholders. We recognise that the law states that this type of data needs more protection. Therefore, data users must be more careful with the way in which we process sensitive personal data.

The school recognises that in addition to sensitive personal data, we are also likely to process information about our stakeholders which is confidential in nature, for example, information about family circumstances, child protection or safeguarding issues. Appropriate safeguards will be implemented for such information, even if it does not meet the legal definition of sensitive personal data.

Biometric Data

The school processes some biometric data as part of an automated biometric recognition system. Biometric data is a type of sensitive personal data.

The school will consider any guidance or advice issued by the Department for Education on the use of biometric data from time to time, applying it as required. The school will obtain the explicit consent of staff, governors, or other Data Subjects before processing their biometric data.

Criminal convictions and offences

There are separate safeguards in the GDPR for personal data relating to criminal convictions and offences. It is possible that the school will process data about criminal convictions or offences. This may be as a result of pre-vetting checks we are required to undertake on staff and governors or due to information which we may acquire during the course of their employment or appointment. In addition, from time to time we may acquire information about criminal convictions or offences involving pupils or parents. This information is not routinely collected and is only likely to be processed by the school in specific circumstances, for example, if a child protection issue arises or if a parent / carer is involved in a criminal matter. Where appropriate, such information may be shared with external agencies such as the child protection team at the local authority, the Local Authority Designated Officer and / or the police. Such information will only be processed to the extent that it is lawful to do so and appropriate measures will be taken to keep the data secure.

Transparency

One of the key requirements of the GDPR relates to transparency. This means that the school will keep Data Subjects informed about how their personal data will be processed when it is collected. One of the ways we provide this information to individuals is through a privacy notice which sets out important information what we do with their personal data. The school wishes to adopt a layered approach to keeping people informed about how we process their personal data. This means that the privacy notice is just one of the tools we will use to communicate this information. Employees are expected to use other appropriate and proportionate methods to tell individuals how their personal data is being processed if personal data is being processed in a way that is not envisaged by our privacy notices and / or at the point when individuals are asked to provide

their personal data, for example, where personal data is collected about visitors to school premises or if we ask people to complete forms requiring them to provide their personal data.

Consent

The school will only process personal data on the basis of one or more of the lawful bases set out in the GDPR, which include consent. Consent is not the only lawful basis and there are likely to be many circumstances when we process personal data and our justification for doing so is based on a lawful basis other than consent. A Data Subject consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. In the event that we are relying on consent as a basis for processing personal data about pupils, if a pupil is aged under 13, we will need to obtain consent from the parent(s). In the event that we require consent for processing personal data about pupils aged 13 or over, we will require the consent of the pupil, and the school re-captures consents from each year group as they start Year 9 – the earliest point where all students will be 13 years of age.

Consent is likely to be required if, for example, the school wishes to use a photo of a pupil on its website or on social media. Consent is also required before any pupils are signed up to online learning platforms. Such consent must be from the parent if the pupil is aged under 13. When relying on consent, we will make sure that the child understands what they are consenting to, and the various consequences of both giving and withholding consent. We will not exploit any imbalance in power in the relationship between us.

Specified, explicit and legitimate purposes

The school will try to be clear with Data Subjects about why their personal data is being collected and how it will be processed. We will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have consented where necessary.

Adequate, relevant and limited to what is necessary

The school will ensure that the personal data collected is adequate to enable us to perform our functions and that the information is relevant and limited to what is necessary. In order to ensure compliance with this principle, the school will check records at appropriate intervals for missing, irrelevant or seemingly excessive information and may contact Data Subjects to verify certain items of data. We will look to minimise requests for information to those necessary. The school will implement measures to ensure that personal data is processed on a 'Need to Know' basis. This means that the only members of staff or governors who need to know personal data about a Data Subject will be given access to it and no more information than is necessary for the relevant purpose will be shared. In practice, this means that the school may adopt a layered approach in some circumstances, for example, members of staff or governors may be given access to basic information about a pupil or employee if they need to know it for a particular purpose but other information about a Data Subject may be restricted to certain members of staff who may need to know it, for example, where the information is sensitive personal data. **It is to be noted that this principle may in some circumstances mean a member of staff is unaware of information which it would have been, in hindsight, helpful to know.**

When personal data is no longer needed for specified purposes, it will be deleted or anonymised in accordance with the school's data retention guidelines (see Annex).

Accurate and, where necessary, kept up to date

If a Data Subject informs the school of a change of circumstances their records will be updated as soon as is practicable.

Where a Data Subject challenges the accuracy of their data, the school will mark the record as potentially inaccurate, or 'challenged'.

In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Data Protection Officer for their judgement. If the problem cannot be resolved at this stage, the Data Subject should refer their complaint to the Information Commissioner's Office. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

Notwithstanding paragraph 8.3, a Data Subject continues to have rights under the GDPR and may refer a complaint to the Information Commissioner's Office regardless of whether the procedure set out has been followed.

Data to be processed in a manner that ensures appropriate security of the personal data

We will develop, implement and maintain safeguards appropriate to our size, scope, our available resources, and the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will periodically evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.

Data users are responsible for protecting the personal data we hold. Data users must implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Data users must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure. **An annex details our expectations of staff, as does our acceptable use policy.**

Data users must follow all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction. Data users must comply with all applicable aspects of our policy and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect personal data.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

Confidentiality means that only people who are authorised to use the data can access it.

Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

Availability means that authorised users should be able to access the data if they need it for authorised purposes.

It is the responsibility of all members of staff and governors to work together to ensure that the personal data we hold is kept secure. We rely on our colleagues to identify and report any practices that do not meet these standards so that we can take steps to address any weaknesses in our systems. Anyone who has any comments or concerns about security should notify the Headteacher or the DPO.

Storing and Protecting Information

To ensure that all data can still be accessed in the event of a security breach and to prevent any loss or theft of data, we will routinely conduct a daily 'encrypted' backup of information and files from our in-house servers and MIS system to the Redstor Cloud service.

Processing in line with Data Subjects' rights

Data Subjects have rights when it comes to how we handle their personal data.

These include rights to:

- withdraw consent to processing at any time;
- receive certain information about the Data Controller's processing activities;

- request access to their personal data that we hold;
- prevent our use of their personal data for direct marketing purposes;
- ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
- restrict processing in specific circumstances;
- challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which personal data is transferred outside of the EEA;
- object to decisions based solely on automated processing, including profiling (Automated Decision Making);
- prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;
- be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority (the ICO); and
- in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

We are required to verify the identity of an individual requesting data under any of the rights listed above. Members of staff should not allow third parties to persuade them into disclosing personal data without proper authorisation.

Webcams and CCTV

The school uses CCTV for security and safety. This is to:

- protect the school buildings and their assets;
- increase personal safety and reduce the fear of crime;
- support the police in a bid to deter and detect crime;
- assist in identifying, apprehending and prosecuting offenders;
- provide evidence for the school to use in its internal investigations and / or disciplinary processes in the event of behaviour by staff, pupils or other visitors on the site which breaches or is alleged to breach the school's policies;
- protect members of the school community, public and private property; and
- assist in managing the school.

The only people with access to this are designated ICT, site management, senior management, and boarding staff. The school has a separate CCTV policy available on request from the Site Manager. Notification of CCTV use is displayed at the front of the school.

We do not use publicly accessible webcams in day school. The use of webcams in boarding to facilitate Skype contact with parent is under review.

Webcams will not be used for broadcast on the internet without prior parental consent.

Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document).

Webcams include any camera on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices.

Please refer to the school CCTV annex for more information.

Incident Reporting

Any breaches of information security where information has been lost or is thought to be lost or inadvertently disclosed must be reported to the DPO.

Any other breaches of the policy or incidents where a member of staff has concern that inadvertent action may leave them vulnerable to a perception that they have broken the policy, should be reported to the Network Manager.

Students in the same circumstance must report what has happened to their teacher or boarding staff.

Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

For all staff, any policy breach may be grounds for disciplinary action in accordance with the school disciplinary procedure. For support staff a breach might also lead to termination of employment or other action within a member of staff's probationary period.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's power to issue monetary penalties was enhanced by GDPR, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the law.

The data protection powers of the Information Commissioner's office are to:

- Conduct assessments to check organisations are complying with the GDPR.
- Serve information notices requiring organisations to provide the Information Commissioner's office with specified information within a certain time period.
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law.
- Prosecute those who commit criminal offences under the Act.
- Conduct audits to assess whether organisations' processing of personal data follows good practice.
- Report to parliament on data protection issues of concern.

For pupils, reference will be made to the school's behaviour policy.

An Annex details how the school responds to suspected data breaches.

Safe use of technology for learning

Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On-demand TV and video, movies and radio/Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT (particularly web-based resources), are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies and that some have minimum age requirements, usually 13 years.

At St George's School, we understand the responsibility to educate our pupils in online safety issues, teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Our comprehensive internet safety policy provides a safe environment to learn and work. The policy includes the following measures:

- Filtered and secure broadband connectivity: The school's internet connection is filtered through a Fortigate filtering system, which blocks sites in categories such as pornography, race hatred, gaming and illegal content. All changes to the filtering policy are logged.
- Monitoring system: The school has installed a FortiAnalyser monitoring system that alerts the Designated Safeguarding Person (DSP) to any safeguarding concerns. The DSP will take appropriate action as necessary.
- Network health: The school uses anti-virus software and strict firewall rules to ensure the health of its network.

List of Annexes:

ANNEX A: Guidance on staff professional responsibilities in their work away from students

1. Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. The school gives relevant staff access to its Management Information System, with a unique username and password.

Always use your own personal passwords**.**

Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers.

Staff should change temporary passwords at first log on.

Do not record passwords or encryption keys on paper or in an unprotected file.

Only disclose your personal password to authorized ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.

If you are aware of a breach of security with your password or account, inform the ICT network office immediately. Change passwords whenever there is any indication of possible system or password compromise.

Passwords can usefully contain a mixture of upper and lowercase letters, numbers and symbols.

Passwords should be changed regularly.

The following website may help to generate passwords: https://passphrase-generator.com/

The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

2. Managing E-mail

The school gives all staff their own e-mail account to use for all school business as a work-based tool. This is to protect staff, minimize the risk of receiving unsolicited or malicious e-mails, and avoids the risk of personal profile information being revealed.

- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged. If necessary, e-mail histories can be traced. The school email account should be the account that is used for all school business.

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.

- The school requires a standard disclaimer to be attached to all e-mail correspondence. The network office will apply this to all school accounts.

- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

- Staff sending e-mails to pupils only outside of EduLink are required to cc the email to the checkmail account (checkmail@stgeorges.herts.sch.uk) unless another colleague has

already been copied in. There is no requirement when emailing parents, but contact with them should be recorded e.g. on CPOMS or SIMS communication log.

- Pupils may only use school-approved accounts on the school system and only under staff supervision for educational purposes and boarder communication.

- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act or a Data Protection Act Subject Access Request. You must therefore actively manage your e-mail account as follows:

    - Delete all e-mails of short-term value.
    - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives.
    - Ensure that emails which need retention are carefully preserved. All others should be permanently deleted. Set up retention policies on folders to ensure this is done.
    - A whole school retention policy will systematically delete e-mails older than 13 months for both staff and students. School Critical email accounts are exempt from this.

- All pupil e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour, particularly in relation to the use of appropriate language, not revealing any personal details about themselves or others in e-mail communication or arranging to meet anyone without specific permission, and not recklessly opening attachments without being sure of their safety.

- Staff must inform the ICT network office if they receive an offensive e-mail or repeated spam or have grounds to believe their account has been compromised, hacked or cloned.

- Pupils are introduced to e-mail as part of the Computing programme of study.

- Pupils must immediately tell a teacher/trusted adult if they receive an offensive or upsetting e-mail on their school account.

- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

3. Sending E-mails

Use your own school e-mail account so that you are clearly identified as the originator of a message.

Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate. We work in what is sometimes a stressful profession and anything we can do as a "stress-buster" should be welcomed. Staff should use their measured professional judgement when deciding on the recipients for an email. Do not copy or forward the e-mail to any more recipients than is absolutely necessary. Please use "All Staff" email group for essential items of information only, not as a discussion forum or to sell items.

Do not send or forward attachments unnecessarily.

School e-mail is not to be used for personal advertising.

4. Receiving E-mails

Check your e-mail regularly during your normal working week.

Activate your 'out-of-office' notification when away for extended periods.

Never recklessly open attachments from an unfamiliar source; consult the Network Manager first.

Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.

The automatic forwarding of e-mails to a non St George's account is not allowed. Forwarding non St George's account (eg personal emails) to a St George's account is also forbidden.

E-mailing what you judge to be highly confidential Information:

Where your conclusion is that e-mail must be used to transmit such data and that it merits the label "highly confidential":

Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

- Encrypt and password protect
- Verify the details, including accurate e-mail address, of any intended recipient of the information.
- Verify (by phoning) the authenticity of a requester before responding to e-mail requests for information.
- Do not send the information to any person whose details you have been unable to separately verify (usually by phone).
- Send the information as an encrypted or password protected document **attached** to an e-mail.
- Provide the encryption key or password by a **separate** contact with the recipient(s), or use a password known commonly within the institution if only basic security is needed
- Make sure any unique password has the normal level of diligence – eight characters, letters and numbers etc.
- Do not identify such information in the subject line of any e-mail.
- Request confirmation of safe receipt.

Personal or Sensitive Information

5. Protecting Personal, Sensitive and Highly Confidential Information

Ensure that any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.

Ensure the accuracy of any personal, sensitive, and highly confidential information you have professional cause to disclose or share with others.

Ensure that personal, sensitive, and highly confidential information is not disclosed to any unauthorized person.

Ensure the security of any personal, sensitive and highly confidential information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment.

Attend to the need not to leave in public view sensitive student information. While a "clear desk" policy is not required in all private work spaces, highly confidential material must be secured out of view from those who might access the space but do not need to know e.g. cleaning or site staff.

Confidential information should only be posted on the wall of office spaces where there is a compelling reason to do so, e.g. medical information which staff need to know to safeguard students at high risk.

Only download personal data from systems for sound professional reasons connected to your duties.

You must not post on the internet personal, sensitive, or highly confidential information, or disseminate such information in any way that may compromise its intended restricted audience.

Be mindful of the need to keep your screen display out of direct view of any third parties when you are accessing personal, sensitive or highly confidential information. Use settings to auto lock your screen if you do nothing for some minutes. Avoid using "Presenter Mode" on a screen where you access sensitive information.

Ensure hard copies of highly confidential or sensitive data are securely stored and disposed of after use in confidential waste.

6. Storing/Transferring Personal, Sensitive or Highly Confidential Information Using Removable Media

Ensure you use password or encryption protected media.

Store all removable media securely.

Securely dispose of removable media that may hold personal data with the assistance of the ICT network office.

Encrypt all files containing information which you judge to be sensitive or highly confidential data.

7. Remote Access from Home or Mobile Media

You are responsible for all activity via your remote access facility.

Only use equipment with an appropriate level of security for remote access.

To prevent unauthorized access to school systems, keep all log-on IDs and PINs confidential and do not disclose them to anyone.

Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.

Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment.

8. Governors

Governors are likely to process personal data when they are performing their duties, for example, if they are dealing with employee issues, pupil exclusions or parent complaints. Governors should be trained on the school's data protection processes as part of their induction and should be informed about their responsibilities to keep personal data secure. This includes:

- Ensure that personal data which comes into their possession as a result of their school duties is kept secure from third parties, including family members and friends.
- Ensure they are provided with a copy of the school's Data Security Policy.
- Using a school email account for any school-related communications.

- Ensuring that any school-related communications or information stored or saved on an electronic device or computer is password protected (and encrypted if highly sensitive).

- Taking appropriate measures to keep personal data secure, which includes, ensuring that hard copy documents are securely locked away so that they cannot be accessed by third parties.

- Governors will be asked to read and sign an Acceptable Use Agreement.

9. Providing information over the telephone

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal data held by the school whilst also applying common sense to the particular circumstances. In particular they should:

I. Check the caller's identity to make sure that information is only given to a person who is entitled to it.

II. Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

III. Refer to their line manager or the DPO for assistance in difficult situations. No-one should feel pressurised into disclosing personal information.

Safe Use of Images

10. Taking of Images and Film

Digital images are easy to capture, reproduce, publish and therefore misuse.

St George's School community is keen to involve and engage students, parents and alumni in all aspects of school life. Actively using social media such as the school Facebook page, e-newsletter, blogs from sports events or trips, Twitter and Instagram, is an important mechanism to achieve this. Realistically, some opportunities to capture images may come when staff only have access to their own devices rather than school hardware.

St George's School views it as appropriate for staff to use their own devices to capture and store imagery taken in the course of school activities both on and off-site so long as it is done in an appropriate and transparent way. Staff should avoid taking images in any private one to one setting. Mindful of the investment that staff make in providing opportunities which staff and students embark upon together, such as trips, sports activities, concerts, productions, house events, prefect and boarding dinners etc., the school endorses that staff may retain such imagery, on condition that any and all such retained images or film may be liable to scrutiny on demand by the school. It is best practice to archive any photos containing students rather than they be kept on a mobile device.

Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of staff unless this is done in the same appropriate and transparent way which binds any imagery taken by staff of students.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

11. Consent to use of named imagery

Parents (students in the case of those aged 13 or over) are specifically asked for permission for the use of imagery on the range of school social media accounts. It is our normal routine for all students to be re-consented at the start of year 9 (the point at which all students in a cohort are aged 13 or over).

The most up to date consent form is considered valid but parents and students may amend permission, in writing, at any time. Students aged 13 or over can also give consent on the spot and in person for their image to be captured (and this may lead to its subsequent use across the full range of media) when an opportunity arises in which they wish to be included e.g. a sports team or MVP photo, a group of students in a house activity, a trip party abroad. Students must not join such group image capture unless they consent to its use. This is a temporary amendment to consent, in the moment, and the student's previous formal written consent is then re-instated unless written notice is given to the contrary.

Pupils' full names will not be published publicly alongside their image and vice versa without permission.

12. Visiting online sites and downloading

Users must not use school IT equipment, or personal technology while on duty to:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Adult material that breaches the Obscene Publications Act in the UK
- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation
- Promoting hatred against any individual or group from the protected characteristics above
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

Users must not:

- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts

- Use software or hardware that has been prohibited by the school
- All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.
- The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by the DPO.

ANNEX B: Organisational Leadership, Monitoring, Responding to Incidents and Concerns, Responsibilities of the ICT Department

1. Information security and online safety - Roles and Responsibilities

Online safety is distinct from information security**.**

Information security relates to ensuring we discharge our obligations as an organisation.

Online safety relates to ensuring as far as possible we keep students and employees safe from harm, distress, and temptation to misuse technology or infringe the rights of others.

As online safety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named online safety co-ordinator in this school is Kirsten Robertson who has been designated this role as a member of the senior leadership team and our DSL. All members of the school community have been made aware of who holds this post. It is the role of the online safety lead to keep abreast of current issues and guidance through organisations such as Herts LA, Herts for Learning Ltd, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior management and governors are updated by the Headteacher/online safety lead and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHCE.

2. Relevant Responsible Persons

Senior members of staff should be familiar with information risks and the school's response.

At St George's School, the lead person is the DPO:

- They lead on the information risk assessment.
- They advise school staff on appropriate use of school technology and policy options, but they do not make policy decision.
- They act as an advocate for information risk management.
- They make judgements on the necessity or otherwise for a Data protection Impact Assessment (DPIA), and determine how that will be done case by case.

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff such as assessment records, medical information and special educational needs data. As responsible member of staff, the Data Protection Officer (DPO) will maintain a register capturing as far as is realistic:

- What information is held, and for what purposes.
- What information needs to be protected and how information will be amended or added to over time.

- Who has access to the data and why.
- How information is retained and disposed of.

As a result, this manager is able to manage and address risks to the information and make sure that information handling complies with legal requirements. In a secondary school, there may be several individuals whose roles involve such responsibility.

However, it should be clear to all staff that the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Negligence of taking reasonable actions to secure data could amount to gross misconduct or even legal action.

Authorized ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice.

ICT authorized staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law.

This may be to confirm or obtain school business-related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the GDPR 2018, or to prevent or detect crime.

ICT authorized staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by authorized staff and comply with the GDPR 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using school ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

The accessing and appropriate use of school data is something that the school takes very seriously.

ANNEX C: Curriculum Guidance

Online safety is fully embedded within our curriculum. The school provides a comprehensive age-appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The PSHE curriculum, Relationships and Health Curriculum are central in supporting the delivery of online safety education as is provision such as the Friday 5 Programme and tutor-led sessions and house assemblies.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment
- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives)
- Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online
- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others
- Understanding the permanency of all online postings and conversations
- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.
- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.
- How the law can help protect against online risks and abuse

ANNEX D: Guidance on Staff Professional Responsibilities in work with Students

1. Managing student use of the Internet

The school provides pupils with filtered access to internet resources (where reasonable) through the school's fixed and mobile internet connectivity.

Staff will preview any sites, online services, software and apps that they actively recommend to students. Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Staff have limited scope to trial new software and providers which hold student level data as part of their service, but if adopted, the DPO must be informed by the end of the academic year so that use of the platform can be incorporated into the school Privacy Notice. If internet research is set for homework, specific sites will be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources.

Staff should consult the DPO before undertaking blogs, wikis etc, in order to take advice on the best platforms to use.

When working with pupils, searching for images should be done through Google Safe Search (standard through the school internet filtering service), Google Advanced Search or a similar application that provides greater safety than a standard search engine. Searching for images through open search engines is discouraged when working with pupils.

If internet research is set for homework, staff work on the reasonable assumption that parents will only allow their child to work on filtered internet settings which would prevent them accessing inappropriate material for their age or understanding.

All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

2. Managing Other Online Technologies

Online technologies, including social networking sites if used responsibly both outside and within an educational context can provide easy-to-use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

At present, the school endeavours to deny access to social networking and online games websites to pupils within day school. 6th form students have more freedom to use their own devices and connectivity, and may therefore be able to circumvent filtering and barriers.

All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.

Pupils are taught to use careful judgement before placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/home phone numbers, school details, email address, specific hobbies/ interests).

Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals, including being mindful of app features which might enable others to track their movements.

Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online.

Our pupils are asked to report any incidents of cyberbullying to their tutor or head of house, and to supply any evidence they can to substantiate claims.

Services such as Facebook and Instagram have a 13+ age rating which should not be ignored.

ANNEX E: STAFF, GOVERNOR, VOLUNTEER, VISITOR TRAINING

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

New staff are provided with a copy of the online safety policy, training in how online safety works at St George's and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with pupils.

ANNEX F: Working in partnership with parents

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.

It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and by other means.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for pupils.

- Parents may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

- Parents should not assume that pupils can bring technological devices to school and should make their child aware of legitimate ways they can contact home in an emergency, such as asking to use a house office or reception office phone

- All cyberbullying incidents affecting children in the school should be reported immediately (if the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection). The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.

- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents and students, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.

- Any parent distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school can impact on the reputation of the whole school community and the welfare of its members. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents.

The school will make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information.

The school will regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents are encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

School action when it becomes aware of concerning content about the school and its staff on social media can include

- Establishing if the material posted constitutes an allegation against a member of staff or a pupil, as if these are of a serious nature, these will need to be formally investigated. This may involve the police and the Headteacher will need to follow the school's safeguarding procedures.

- If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice may be sought.
- Contacting complainants and inviting them to a meeting. Such a meeting would draw attention to the seriousness and impact of the issue being raised in the manner chosen by that party and
    1. Ask for the offending remarks to be removed;
    2. Explore the complainant's grievance;
    3. Agree next steps;
    4. Clarify the correct complaints procedures.

  If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

    - Reporting the matter to the social network site if it breaches their rules or breaks the law;
    - Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, the issue will be escalated accordingly.

ANNEX G: STAFF USE OF SOCIAL MEDIA GUIDANCE

Staff may only include any image of a student in a personal online platform, even unnamed, if that image has already been posted on an official school portal such as the school website, blog, or similar.

Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Data Protection Officer.

Staff should not make person to person non-transparent social contact with students on social networking sites – email contact should always be conducted through the member of staff's school email address and be copied to Checkmail.

It would be unusual for a member of staff to have cause to use a personal social media account to "follow" any individual current student or student's social media posts, be it Facebook, X, Instagram, or any other similar platform. Any colleague would be expected to give full account of the reason for any such interaction, and would need to be mindful of the way motives or actions could be misconstrued.

Any staff using social networking sites such as Facebook or X should ensure their privacy settings are set to the highest level.

In terms of staff personal usage of Facebook, the following safeguards are to be observed by all staff:

- An appropriate boundary must be set between personal and professional life while using social media.
- Use your discretion when dealing with friend requests from parents. It is acceptable to decline these invitations and explain why they should use formal professional means of contact.
- Realise that pupils will be naturally curious about your personal life outside school and may try to find out more about you. Manage your privacy setting and keep them under review. These are particularly important in regard to photos and videos, and remember that no privacy mechanism is 100% guaranteed.
- Ensure your settings prohibit others from tagging you in any photos or updates without your permission and you can ask others to remove any undesirable content related to you.
- Audit and re-evaluate the information about you and who has access to it if you are joining the profession through an Initial Teacher Training route or returning to work after an absence.
- Consider that conversations held online may not be private. Be aware of who may have access to what you post – you should only post to 'Friends' by default rather than 'Friends of Friends' and ensure that people on your 'Friends' list are appropriate to view your personal content. You should always assume that information you post can be accessed and altered.
- Do not discuss pupils, colleagues, parents or carers online or criticise your employer or others within the school community; respect pupil privacy and confidentiality at all times.

If staff are 'friends' with ex-students, they must be aware of their professional conduct and not make themselves vulnerable by sharing content that would cause issues if within in the public domain. Staff should also be aware of parents who are in their social network and consider their conduct accordingly.

In general, professional and confidential matters relating to school should not be posted on social media except through official school accounts.

The previous advice and practice for Facebook equally applies to Twitter, but there are a number of additional statements with respect to this platform:

- Photographs of students will only be used if a parent/carer (or student aged 13 or over) has granted permission.

- Open tweets from followers may be replied to and positive debate encouraged.

- Students and parents/carers will not be 'followed' by ANY school account. Furthermore, school Twitter accounts will not be used to send 'direct messages'.

- Students will not be allowed to follow staff member's personal accounts. Staff members should review their lists of followers and block any current St George's students.

- Care must be taken by staff when expressing political views or controversial opinions, even in the context of encouraging debate and critical thinking. These statements could be misconstrued when taken out of context. **Content should only be posted if appropriate for a classroom environment and a public setting. E-mail, texting and social media encourage casual dialogue and often innocent actions can easily be misconstrued or manipulated.**

Electronic messages are not anonymous and can be tracked and live forever on the internet. Social media sites archive content posted, even when deleted from online profiles. Once information is placed online, the author relinquishes control of it. Staff should never share information with students in ANY environment that they would not willingly or appropriately share in a school or school-related setting or in the community.

In summary, staff need to be aware of their 'Digital Footprint' and ensure that any online media attributable to them is appropriate in their professional context. Platforms such as Snapchat and Instagram, Tinder and Grindr require particular care!

In use of Snapchat, staff should make sure they are using the default setting to accept only incoming and sent pictures from/to 'My Friends.' Staff should be mindful that recipients can "screen grab" Snapchat images, and only post sensibly.

This need for care applies retrospectively; therefore staff joining the school should review publicly available media referring to them (e.g. blogs, photos, videos) and ensure that the content could not lead to disrepute for the staff member or school.

Some specific points on electronic communication:

- Staff should be aware that postings on social media can be used in a defamation claim.

- Staff should be mindful that what seems to one staff member as a 'bit of banter' may seem to another a gross and harassing intrusion into their private space or cause possible alarm and or distress.

- It is important that no communication with a student may in anyway take advantage of a position of trust or breach their duty of care, regardless of the medium of this communication.

The following examples are not exhaustive, but would be considered to be at least a breach of school direction and may also be criminal in some cases:

- Inappropriate electronic communication with pupils, colleagues and parents/carers, including SMS and instant messaging.

- Posting/sending sexually explicit pictures/images to colleagues or pupils.

- Grooming - whereby a teacher uses electronic messages with a view to establishing an inappropriate relationship with a pupil.

- Posting content that could bring the profession or the school into disrepute.

Any member of staff aware of an inappropriate message or film that could lead to hurt, distress for a student or colleague or bring the school into disrepute in the public domain should report the matter, at the earliest convenience, to a senior member of staff.

Bring the matter to the attention of a member of the leadership group if you are the victim of cyber bullying or uncomfortable with comments, photos or posts made by pupils of or about you. Whistleblowing is the mechanism by which staff can voice their concerns, made in good faith, without fear of repercussion. It is a member of staff's responsibility to report any behaviour by colleagues that raises concern. Staff should report concerns to a member of the leadership group or in the case of a complaint about the Headteacher, to the Chair of Governors.

ANNEX H: ACCEPTABLE USE AGREEMENT:
STAFF including SUPPLY STAFF, GOVERNORS, VOLUNTEERS, AND VISITORS

Code of Conduct

This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with the relevant Deputy Head.

- I will only use the school's email/internet/intranet/learning platform and any related technologies for professional purposes or for reasonable uses within the bounds of the school policy.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils except for a transparent professional cause.
- I will only use the approved, secure e-mail system(s) for any school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act (some supply staff or volunteers may not be issued a school email address, and must be mindful of the lower levels of security which may apply to using other email platform out of necessity for limited school based work).
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely for valid professional reasons. Personal or sensitive data taken off site must be secured, e.g. on a password secured laptop or memory stick.
- I will ensure that any non-work related usage of school ICT equipment or the Wi-Fi network or my own devices will be limited to what is reasonable and does not conflict in any way with my professional responsibilities or duties.
- I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Headteacher.
- I will not install any hardware or software without permission of the ICT network office.
- I will not browse, download, upload or distribute any material that could be considered by a reasonable person to be offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy.
- Images will not be distributed outside the school network such as on social media without proper consideration of issues of appropriateness and safeguarding.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could be reasonably foreseen to upset any member of the school community.

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my line manager or the Headteacher. I will respect copyright and intellectual property rights.

- I will take reasonable care to ensure that my online activity, both in school and outside school, will not bring the school, my professional role or that of others into disrepute. I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils. While the school recognises my legitimate right to have a private life outside school, I will not engage in conduct outside work which could reasonably be expected to seriously damage the school or my own reputation or that of other members of the school community.

- When using social networking for personal use I will ensure my settings are not public. Privileged information must remain confidential.

- I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DPO and DSL. A school-owned device should be used when running video-conferences, where possible.

- I will support and promote the school's online safety and information security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

- I understand this forms part of the terms and conditions set out in my contract of employment. I have made myself familiar with the annexes which accompany the school policy such as they apply to my role and will stay within their terms.

- I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, pupils or parents/carers) to the DSL (for student concerns) and to the Headteacher (for concerns about staff).

- I understand that if I fail to comply with this Acceptable Use Agreement I could be subject to disciplinary action. This could include a warning, a suspension, removal from a volunteer role or supply work for the school, referral to governors and/or the local authority and in the event of illegal activities the involvement of the police.

User Signature

I agree to follow this Code of Conduct and to support the safe and secure use of ICT throughout the school.

Full Name: …… Date: ……

Job Title: ..…….....

Signature: …….. (Printed)

ANNEX I: Student on-line safety acceptable use agreement

1. I will not download or install software on school IT equipment.
2. I will only log on to the school network, other school systems and resources using my own school username and password.
3. I will not reveal my passwords to anyone other than a parent/carer.
4. I will not use my personal email address or other personal accounts on school IT equipment.
5. I will make sure that all my electronic communications are responsible and sensible. I understand that the school discipline policy allows staff to take action if my internet use is illegal and / or offensive, even if that activity takes place away from the school site, day, week, and term.
6. I understand my behaviour in the virtual classroom should mirror that in the physical classroom.
7. I understand that everything I search for, access, post or receive online can be traced now and in the future. My activity can be monitored and logged and if necessary shared with teachers, parents/carers and the police if necessary. I know it is essential that I build a good online reputation.
8. I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to a member of staff if I am in school, or parent if I am not in school.
9. I will not give out my own or others' personal information, including: name, phone number, home address, interests, schools or clubs or any personal image. I will report immediately any request for personal information, to a member of staff if I am in school or parent if I am not in school.
10. I should never post photographs, videos or livestream without the permission of all parties involved.
11. I will not upload any images, videos, sounds or words that **could** be expected to upset, now or in the future, any member of the school community, as this is cyberbullying.
12. I will be respectful to everyone online; I will treat everyone the way that I want to be treated. I will ensure that all my online activity, both in and outside school, will not cause distress to anyone in the school community or bring the school into disrepute.
13. I will not respond to hurtful behaviour online but will report it. I have the right to block and will say no to any inappropriate or upsetting request.
14. I will respect the privacy and ownership of others' work on-line and will adhere to copyright at all times.
15. I will not attempt to bypass the internet filtering system in school.
16. I will not assume that new technologies can be brought into school and will check with staff before bringing in any device.
17. I will not lie about my age in order to sign up for age-inappropriate games, apps or social networks.
18. I understand that not everything I see or hear online is true, accurate or genuine. I also know that some people on the internet are not who they say they are and may have ulterior motives for assuming another identity that will put me at risk. I will gain permission from parents before arranging to meet someone I only know on the internet.
19. I understand that these rules are designed to keep me safe now and in the future. If I break the rules, teachers will investigate, I may be disciplined and my parents/carers may be contacted. If I break the law the police may be informed.

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community, the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

1. Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.

2. Incidents should be reported immediately. Pupils should report to their child's Head of House and staff members should seek support from the Deputy Head and/or DSL.

3. The person reporting the cyberbullying should save the evidence and record the time and date. This evidence should not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff will not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the Headteacher so that the circumstances can be recorded.

4. A senior member of staff will meet with the person who has reported the incident and the victim, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.

5. A senior member of staff will conduct an investigation.

6. Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime. The school discipline policy details the school based consequences which may follow.

7. Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

ANNEX J: ON-LINE SAFETY INCIDENTS AND INFRINGEMENTS

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised. All staff have the individual responsibility to ensure that incidents have been correctly acted upon and reported.

Online internet incidents are automatically logged by our firewall and filtering solution "Fortigate" and acted on by the network manager or the DSP.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Any incidents involving cyberbullying will also need to be recorded on CPOMS: the relevant Head of House needs to be advised.

Type of incident(s) (indicate as many as apply)	
Accessing age inappropriate websites, apps and social media	Accessing someone else's account without permission
Forwarding/spreading chain messages or threatening material	Posting images without permission of all involved
Online bullying or harassment (cyberbullying)	Posting material that will bring an individual or the school into disrepute
Racist, sexist, homophobic, religious or other hate material	Online gambling
Sexting/Child abuse images	Deliberately bypassing security
Grooming	Hacking or spreading viruses
Accessing, sharing or creating pornographic images and media	Accessing and/or sharing terrorist material
Accessing, sharing or creating violent images and media	Drug/bomb making material
Creating an account in someone else's name to bring them into disrepute	Breaching copyright regulations
Other breach of Acceptable Use Agreement	

Immediate action taken following the reported incident:
Incident reported to online safety Lead /DSP/Headteacher
Safeguarding advice sought, please specify
Referral made to HCC Safeguarding
Incident reported to police and/or CEOP
Online safety policy to be reviewed/amended
Parent(s)/carer(s) informed please specify
Incident reported to social networking site
Other actions e.g. warnings, sanctions, debrief and support
Response in the wider community e.g. letters, newsletter item, assembly, curriculum delivery

The nature and outcomes section might usefully consider these possible options

Misuse and Infringements, whether wilful, reckless, negligent, or inadvertent

Complaints

Complaints and/or issues relating to online safety or information security should be made to the DPO who will determine the members of staff who can best consider the issue and respond.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. **The breach must be immediately reported to the ICT network office.**

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation or other process as determined by the Headteacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart).

- Any information-gathering about an incident will attempt to ascertain whether an infringement **is wilful, reckless, negligent, or inadvertent**. The response of the person concerned in making others aware of the breach, is one factor in determining this. Other considerations include, but are not limited to, the context, the technical understanding of the person, any previous issues and technical evidence and so on.

- Users are made aware of sanctions relating to the misuse or misconduct through this policy, and the discipline policy relevant to them as a student or member of staff.

ANNEX K: Data Protection Officer

The DPO is responsible for monitoring compliance with current data protection law, and has the knowledge, support and authority to do so effectively. They oversee the school's data protection processes and advise the school on best practice.

The DPO for St George's School is Mr J. Day, Assistant Headteacher. He is supported in some tasks by Mrs S. Jackson, Data Manager.

The DPO acts to:

- Advise the school and its employees about their obligations under current data protection law, including the General Data Protection Regulation (GDPR).
- Develop an in-depth understanding of the school's processing operations, information systems, data security processes and needs, and administrative rules and procedures.
- Monitor the school's compliance with data protection law, by:
    - Collecting information to identify data processing activities.
    - Analysing and checking the compliance of data processing activities.
    - Informing, advising and issuing recommendations to the school.
    - Ensuring they remain an expert in data protection issues and changes to the law, attending relevant training as appropriate.
- Ensure the school's policies are followed, through:
    - Assigning responsibilities to individuals.
    - Awareness-raising activities.
    - Coordinating staff training.
    - Conducting internal data protection audits.
- Advise on and assist the school with carrying out data protection impact assessments, if necessary.
- Act as a contact point for the Information Commissioner's Office (ICO), assisting and consulting it where necessary, including:
    - Helping the ICO to access documents and information.
    - Seeking advice on data protection issues.
- Act as a contact point for individuals whose data is processed (for example, staff, pupils and parents), including:
    - Responding to subject access requests.
    - Responding to other requests regarding individuals' rights over their data and how it is used.
- Take a risk-based approach to data protection, including:
    - Prioritising the higher-risk areas of data protection and focusing mostly on these.
    - Advising the school if/when it should conduct an audit, which areas staff need training in, and what the DPO role should involve.
- Report to the governing body on the school's data protection compliance and associated risks.
- Respect and uphold confidentiality, as appropriate and in line with data protection law, in carrying out all duties of the role.

- Undertake any additional tasks necessary to keep the school compliant with data protection law and be successful in the role.

The DPO reports in the first instance to the Headteacher. While the DPO will advise the Headteacher and leadership team on issues to do with data policy, strategy and GDPR compliance, the Headteacher is the decision maker in these areas.

Should the DPO post holder's work be called into question, the Headteacher will oversee any necessary process to investigate.

Should the DPO be of the view that decisions of the Headteacher and leadership group amount to a breach of the requirements of the GDPR, the DPO is expected to inform the Chair of Governors, and beyond that post holder the ICO itself.

Annex L: PRIVACY NOTICE

See separate document that can be viewed on school website

Annex M: Deployment of Protective Monitoring Software and 'Reasonable Personal Use'

We recognise that the overwhelming majority of our staff can be trusted to use work systems appropriately and professionally.

Alongside many other schools, St George's allows for the deployment of software that provides the facility to monitor user activity across the entire IT networks in order to protect those systems and to provide a robust audit process. The school reserves **the right to monitor** and carry out dip sampling of e-mail and internet usage by employees, to ensure adherence to this requirements. This may be done at any time with no notice being given. Any content or material found that is deemed to be inappropriate, or not in line with business needs may be used as a basis for disciplinary action.

The facility will allow the school ICT network office, where justified and proportionate, to audit the activity of any user, irrespective of their role, terminal accessed or application used. Users are therefore reminded that whilst using school systems, for any purpose, they will be subject to monitoring however this will be carried out in line with requirements of the Data Protection Act and their Human Rights under Article 8. Note that regardless of the application, passwords are not routinely recorded.

It's important to reassure people that the system will not be used to "spy" on employees but can be used by the network office under the direction of the Headteacher to react to reports of misuse or proactively investigate abuse of our systems. It will greatly speed up investigations and allow early resolution of any question of misuse.

The term Reasonable Personal Use is defined as usage of a system or application, by an employee, during their normal working hours to such an extent that it does not impact upon their work. The final decision on this always rests with the Headteacher. If an employee is in any doubt about how reasonable their personal usage is, they should consult with their line manager. Line managers should be proactive in ensuring that employees adhere to this and should also ensure that as part of any induction package individuals are reminded of St George's stance in relation to what is reasonable.

If any employee has any concerns about having their email monitored then they shall make their concerns known to their line manager, who shall review the concerns with the Network Manager. However, no employee may refuse this requirement as all aspect of the schools systems are provided for the primary and sole purpose of the school's business and operation.

Annex N – Biometric Data Capture and Retention

St George's School operates biometric catering and library systems. This technology has been used successfully by many hundreds of schools and we are convinced that this is the right way for St George's to maintain its high level of service in these two areas, reducing queuing and administration times, and the cash held by students and processed by our finance department.

Biometric information is information about a person's physical or behavioural characteristics that can be used to identify them. The school requests consent to take and use information from the finger of students and staff for the purpose of providing individuals with easy access to the school's cashless catering, and library services. This system takes measurements of an individual's finger and converts these measurements into a template (a string of numbers), which is then encrypted. The data held cannot be used to recreate a fingerprint image, nor can it be used in a forensic investigation.

An image of the individual's fingerprint is not stored. The template is used to permit the individual to access to the catering and library services by placing their finger on a scanner at the point of sale or service. (Please note that this registration also applies to boarders even though meals are included in termly fees).

St George's School will comply at all times with the GDPR and Protection of Freeedoms Act and with the guidance given by Becta and by the Information Commissioner's office regarding the use of biometric data. The law places specific requirements on schools when using personal information, such as biometric information.

In order to be able to use a child's biometric information, the written consent of at least one parent is required. However, consent given by one parent will be overridden if the other parent objects in writing. Similarly, if a child objects, the school cannot collect or use his/her biometric information for inclusion on the automated recognition system. A parent can object in writing to the proposed processing of their child's biometric information at a later stage or withdraw any consent they have previously given. Once an individual ceases to use the biometric recognition system, his/her biometric information will be securely deleted.

Annex O: Cloud Storage

St George's School is committed to ensuring its IT systems are secure, school data and systems are protected and are only accessed by authorised users. All school staff using "Cloud Storage" services must therefore adhere to this.

For this document, the phrase "cloud storage" refers to third party online storage services such as Google Drive, Dropbox and OneDrive. Files stored on these services can usually be accessed via any web browser and often have the capability to be "synchronised" to multiple computers and mobile devices such as mobile phone and tablets. They may also have facilities for sharing files with other people.

Our staff and students are now directed to use school managed cloud storage (Google and 365) linked to their school google/email accounts. This allows convenient access to their files and data from a number of different devices. Other online personal storage for school business is strictly discouraged.

Use of non-school managed services in school work setting introduce risks to the security, privacy, copyright and retention of school data.

To ensure the integrity of information on the cloud storage:

- Creation of Shared areas and Access controls protecting the data on 'Shared Drives' is maintained by senior members of ICT Support
- Should an individual suddenly become ill, be absent for other reasons or leave, the school will permit other staff access to the data if directed by DPO.
- Deleted Files/Folders from school managed cloud services can only be retrieved on Microsoft 365 within 30 days and Google drive within 6 months. No additional backup is undertaken on cloud storage.

The main risks when files are stored in public or school managed cloud storage to take into consideration are that:

- Google, Microsoft, Dropbox, and the other big cloud providers are GDPR compliant, since they can offer their services in the EU. The location where the data is stored may not be guaranteed as remaining in the European Economic Area (EEA) or US Safe Harbour and so may not meet Data Protection Act requirements for personal data in the future.
- Few cloud providers guarantee they will not access the information stored within their service, leading to concerns over privacy and intellectual property rights.
- Some if not all providers do not guarantee that the user's ownership of the data stored in the cloud will be retained. This is primarily to enable the providers to move data around to their different server locations without your prior approval but opens further questions about intellectual property rights.
- Using cloud storage client software to synchronise files between work and personal devices could result in sensitive information being held inappropriately on personal equipment. Only use such software on school owned equipment.
- If they have financial difficulties a cloud storage provider may end the service with little or no notice, leaving users with no access to files. This is less likely with software leaders such as Google and Microsoft.

All staff have a responsibility to protect the school's data, particularly data about individuals:

- Do not use cloud storage to store files containing information about individuals or other sensitive information without limiting access to those staff that need access and password protecting such documents. Refer to the school Data Protection Policy for more information.

- If you are using cloud storage for collaboration with others, either from within the school or elsewhere, only grant access to files or folders that are required for the collaboration to take place. Access to personal data should be given on a strictly need to know basis to comply with the Data Protection Act.
- The school will support 'Google drive for desktop' on school devices, but does not support other cloud storage clients or apps, such as those available for Dropbox.
- Use the Shared area on school servers for current documents in addition to cloud storage.
- You must ensure that there is a suitable level of encryption on any mobile or portable device used to download any data about individuals from cloud storage. Such a device must be password protected.

The school has provided to all staff and students Microsoft Office 365 Email and Google Education accounts. As part of this, members have access to Microsoft 'OneDrive for Business' and 'Google Drive' and other related online services. Microsoft/Google currently store data uploaded by staff/student accounts in EEA or US Safe Harbour locations and comply with current UK GDPR. Using Google Drive via a staff logon ID is recommended cloud solution for our school staff/students.

With a Google School account, you will have access to online Google Office Suite and real time collaboration tools (document sharing, class shared areas instant messaging, video conferencing and social networking).

Your school email Office 365 account will allow you to install the latest desktop versions of Microsoft Word, Excel, PowerPoint, OneNote, Outlook, Access and Publisher on up to 5 personal devices.

St George's School provides secure remote VPN access to school Network resources such as SIMS, home/shared folders (available to key staff) from home on school owned laptops. Remote access will be authorised by the ICT Network Manager.

Annex P: Data Protection Impact Assessments

Checklist to assess if a DPIA is needed

Under the GDPR, data protection impact assessments (DPIAs) are mandatory where the processing poses a high risk to the rights and freedoms of individuals. While they can also be carried out in other situations, organisations need to be able to evaluate when a DPIA is required.

The following checklist helps you make that assessment and provides a springboard for some of the issues you will need to consider in more detail if you do need to carry out a DPIA.

The ICO's draft guidance on DPIAs states, "…the important point here is not whether the processing is actually high risk or likely to result in harm – that is the job of the DPIA itself to assess in detail. Instead, the question is a more high-level screening test: are there features which point to the potential for high risk?"

The school / Trust's DPO must be involved in the process of assessing whether a DPIA is required. The answers below can be used to help inform a decision about whether to carry out a DPIA. If it is unclear if a DPIA is required for the processing activity, it is recommended that one is undertaken to ensure compliance and as a matter of good practice.

The checklist below is not exhaustive and is indicative of the circumstances when a DPIA may be needed, for example, in some circumstances a DPIA should be carried out if only one question is answered affirmatively and in others two or more affirmative answers may lead you to conclude that a DPIA is needed. It is up to the school / Trust to decide if the processing is likely to result in high risk taking into account the nature, scope, context and purposes of the processing

The definition of "Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Criteria	***Answer***
What is the objective/intended outcome of the project?	
Is it a significant piece of work affecting how services/operations are currently provided?	
Who are the data subjects or who will be affected by the project?	
Will the project involve the collection of new information about people? (E.g. new identifiers or behavioural information relating to individuals?)	
Will the project involve combining anonymised data sources in a way that may give rise to a risk that individuals could be identified?	
Will the project involve combining datasets originating from different processing operations or data controllers in a way which would exceed the reasonable expectations of the individuals?	
Is data being processed on a large scale (consider the number of data subjects concerned, the volume of data and/or the range of different data items being processed, the duration of the processing and the geographical extent of the processing)?	

Criteria	*Answer*
Will the project compel individuals to provide information about themselves?	
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
Will personal information be transferred outside the EEA?	
Is information about individuals to be used for a purpose it is not currently used for, or in a way it is not currently used?	
Will information about pupils or other vulnerable persons (e.g. employees) be collected or otherwise processed?	
Will new technology be used which might be seen as privacy intrusive? (e.g. tracking, surveillance, observation or monitoring software, capture of image, video or audio or location)	
Is monitoring or tracking or profiling of individuals taking place?	
Is data being used for automated decision making with legal or similar significant effect?	
Is data being used for evaluation or scoring? (e.g. performance at work, economic situation, health, interests or behaviour)	
Is sensitive data being collected including:	
i. Race	
ii. Ethnic origin	
iii. Political opinions	
iv. Religious or philosophical beliefs	
v. Trade union membership	
vi. Genetic data	
vii. Biometric data (including facial recognition)	
viii. Finger or palm print data	
ix. Health data	
x. Data about sex life or sexual orientation?	
Does the processing include personal data relating to criminal offences or prosecutions?	
Will the processing itself prevent data subjects from exercising a	

Criteria	*Answer*
right or using a service or contract?	
Is the information about individuals of a kind likely to raise privacy concerns or is it information people would consider to be particularly private or confidential?	
Will the project require contact to be made with individuals in ways they may find intrusive?	
Does the project involve new or significantly changed handling of personal data about a large number of individuals?	
Could the processing endanger the individual's physical health or safety in the event of a security breach?	
Does the processing involve collecting personal data from a source other than the individual without providing them with a privacy notice?	
Are you considering a major project which will involve the use of personal data?	

Annex Q: Guidance on retention of data

The school looks to apply the following guidelines from the Information and Records Management Society in retention of different kinds of data:

1.	Child Protection				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
1.1	Child Protection files	Yes	Education Act 2002, s175, related guidance "Safeguarding Children in Education", September 2004	DOB + 25 years [1]	SECURE DISPOSAL
1.2	Allegation of a child protection nature against a member of staff, including where the allegation is unfounded	Yes	Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance) Education Act 2002 guidance "Dealing with Allegations of Abuse against Teachers and Other Staff" November 2005	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	SECURE DISPOSAL

2.	Governors				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
2.1	Minutes				
	• Principal set (signed)	No		Permanent	Retain in school for 6 years from date of meeting
	• Inspection copies	No		Date of meeting + 3 years	SECURE DISPOSAL [If these minutes contain any sensitive personal information they should be shredded]
2.2	Agendas	No		Date of meeting	SECURE DISPOSAL
2.3	Reports	No		Date of report + 6 years	Retain in school for 6 years from date of meeting
2.4	Annual Parents' meeting papers	No		Date of report + 6 years	Retain in school for 6 years from date of meeting
2.5	Instruments of Government	No		Permanent	Retain in school whilst school is open
2.6	Trusts and Endowments	No		Permanent	Retain in school whilst operationally required
2.7	Action Plans	No		Date of action plan + 3 years	SECURE DISPOSAL
2.8	Policy documents	No		Expiry of policy	Retain in school whilst policy is operational (this includes if the expired policy is part of a past decision making process)

2.	Governors				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
2.9	Complaints files	Yes		Date of resolution of complaint + 6 years	Retain in school for the first six years Review for further retention in the case of contentious disputes SECURE DISPOSAL routine complaints
2.10	Annual Reports required by the Department for Education	No	Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.SI 2002 No 1171	Date of report + 10 years	
2.11	Proposals for schools to become, or be established as Specialist Status schools	No			Current year + 3 years

3.	Management				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
3.1	Log Books	Yes		Date of last entry in the book + 6 years	Retain in the school for 6 years from the date of the last entry
3.2	Minutes of the Senior Management Team and other internal administrative bodies	Yes		Date of meeting + 5 years	Retain in the school for 5 years from meeting
3.3	Reports made by the head teacher or the management team	Yes		Date of report + 3 years	Retain in the school for 3 years from meeting
3.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes		Closure of file + 6 years	SECURE DISPOSAL
3.5	Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	No		Date of correspondence + 3 years	SECURE DISPOSAL
3.6	Professional development plans	Yes		Closure + 6 years	SECURE DISPOSAL
3.7	School development plans	Yes		Closure + 6 years	Review
3.8	Admissions - if the admission is successful	Yes		Admission + 1 year	SECURE DISPOSAL
3.9	Admissions - if the appeal is unsuccessful	Yes		Resolution of case + 1 year	SECURE DISPOSAL

3.	Management				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
3.10	Admissions - Secondary Schools - Casual	Yes		Current year + 1 year	SECURE DISPOSAL
3.11	Proofs of address supplied by parents as part of the admissions process	Yes		Current year + 1 year	SECURE DISPOSAL
3.12	Supplementary Information form including additional information such as religion, medical conditions etc.				

4.	Pupils				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
4.1	Admission Registers	Yes		Date of last entry in the book (or file) + 6 years Re consider Retention Period. Feedback from Teaching Relative was thought to be 7 Year Retention. These records are no longer generated in paper but electronically held using SIMS BROCON software.	Retain in the school for 6 years from the date of the last entry then consider transfer to the Archives
4.2	Attendance registers	Yes		Date of register + 3 years	SECURE DISPOSAL [If these records are retained electronically any back up copies should be destroyed at the same time]

4.	Pupils				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
4.3	Pupil Files Retained in Schools	Yes			
4.3a	• Primary			Retain for the time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school. In the case of exclusion it may be appropriate to transfer the record to the Pupil Referral Unit
4.3b	• Secondary		Limitation Act 1980	DOB of the pupil + 25 years [3]	SECURE DISPOSAL
4.4	Pupil files	Yes			
4.4a	• Primary			Retain for the time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school. In the case of exclusion it may be appropriate to transfer the record to the Pupil Referral Unit
4.4b	• Secondary		Limitation Act 1980	DOB of the pupil + 25 years [4]	SECURE DISPOSAL
4.5	Special Educational Needs files, reviews and Individual Education Plans	Yes		DOB of the pupil + 25 years the review NOTE: This retention period is the minimum period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period.	SECURE DISPOSAL

4.	Pupils				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
4.6	Correspondence Relating to Authorised Absence and Issues	No		Date of absence + 2 years	SECURE DISPOSAL
4.7	Examination results	Yes			
4.7a	• Public	No		Year of examinations + 6 years	SECURE DISPOSAL
4.7b	• Internal examination results	Yes		Current year + 5 years [5]	SECURE DISPOSAL
4.8	Any other records created in the course of contact with pupils	Yes/No		Current year + 3 years	Review at the end of 3 years and either allocate a further retention period or SECURE DISPOSAL
4.9	Statement maintained under The Education Act 1996 - Section 324	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending
4.10	Proposed statement or amended statement	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending
4.11	Advice and information to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years	SECURE DISPOSAL unless legal action is pending
4.12	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years	SECURE DISPOSAL unless legal action is pending
4.13	Parental permission slips for school trips - where there has been no major incident	Yes		Conclusion of the trip	SECURE DISPOSAL

4.	Pupils				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
4.14	Parental permission slips for school trips - where there has been a major incident	Yes	Limitation Act 1980	DOB of the pupil involved in the incident + 25 years The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils	SECURE DISPOSAL
4.15	Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Primary Schools	No	3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998).	Date of visit + 14 years [6]	N
4.16	Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Secondary Schools	No	3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998).	Date of visit + 10 years	N
4.17	Walking Bus registers	Yes		Date of register + 3 years This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting	SECURE DISPOSAL [If these records are retained electronically any back up copies should be destroyed at the same time]

5.	Curriculum				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
5.1	School Development Plan	No		Current year + 6 years	SECURE DISPOSAL
5.2	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
5.3	Schemes of work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.4	Timetable	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.5	Class record books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.6	Mark Books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.7	Record of homework set	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.8	Pupils' work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL

5.	Curriculum				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
5.9	Examination results	Yes		Current year + 6 years	SECURE DISPOSAL
5.10	SATS records - Examination Papers and Results	Yes		Current year + 6 years	SECURE DISPOSAL
5.11	PAN reports	Yes		Current year + 6 years	SECURE DISPOSAL
5.12	Value Added & Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL
5.13	Self Evaluation forms	Yes		Current year + 6 years	SECURE DISPOSAL

6.	Personnel Records held in Schools				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
6.1	Timesheets, sick pay	Yes	Financial Regulations	Current year + 6 years	SECURE DISPOSAL
6.2	Staff Personal files	Yes		Termination + 7 years	SECURE DISPOSAL
6.3	Interview notes and recruitment records	Yes		Date of interview + 6 months	SECURE DISPOSAL
6.4	Pre-employment vetting information (including CRB checks)	No	CRB guidelines	Date of check + 6 months	SECURE DISPOSAL [by the designated member of staff]
6.5	Disciplinary proceedings:	Yes	Where the warning relates to child protection issues see 1.2. If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice.		

6.	Personnel Records held in Schools				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
6.5a	• oral warning			Date of warning + 6 months	SECURE DISPOSAL [7]
6.5b	• written warning - level one			Date of warning + 6 months	SECURE DISPOSAL
6.5c	• written warning - level two			Date of warning + 12 months	SECURE DISPOSAL
6.5d	• final warning			Date of warning + 18 months	SECURE DISPOSAL
6.5e	• case not found			If child protection related please see 1.2 otherwise SECURE DISPOSAL immediately at the conclusion of the case	SECURE DISPOSAL
6.6	Records relating to accident/injury at work	Yes		Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL
6.7	Annual appraisal/assessment records	No		Current year + 5 years	SECURE DISPOSAL
6.8	Salary cards	Yes		Last date of employment + 85 years	SECURE DISPOSAL
6.9	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)	Current year +3yrs	SECURE DISPOSAL
6.10	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL

6.	Personnel Records held in Schools				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
6.11	Proofs of identity collected as part of the process of checking "portable" enhanced CRB disclosure	Yes		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file.	

7.	Health and Safety				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
7.1	Accessibility Plans		Disability Discrimination Act	Current year + 6 years	SECURE DISPOSAL
7.2	Accident Reporting		Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
7.2a	• Adults	Yes		Date of incident + 7 years	SECURE DISPOSAL
7.2b	• Children	Yes		DOB of child + 25 years[8]	SECURE DISPOSAL
7.3	COSHH			Current year + 10 years [where appropriate an additional retention period may be allocated]	
7.4	Incident reports	Yes		Current year + 20 years	SECURE DISPOSAL

7.	Health and Safety				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
7.5	Policy Statements			Date of expiry + 1 year	SECURE DISPOSAL
7.6	Risk Assessments	Yes		Current year + 3 years	SECURE DISPOSAL
7.7	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos			Last action + 40 years	SECURE DISPOSAL
7.8	Process of monitoring of areas where employees and persons are likely to have come in contact with radiation			Last action + 50 years	SECURE DISPOSAL
7.9	Fire Precautions log books			Current year + 6 years	SECURE DISPOSAL

8.	Administrative				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
8.1	Employer's Liability certificate			Closure of the school + 40 years	SECURE DISPOSAL
8.2	Inventories of equipment & furniture			Current year + 6 years	SECURE DISPOSAL
8.3	General file series			Current year + 5 years	Review to see whether a further retention period is required
8.4	School brochure or prospectus			Current year + 3 years	
8.5	Circulars (staff/parents/pupils)			Current year + 1 year	SECURE DISPOSAL

8.	Administrative				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
8.6	Newsletters, ephemera			Current year + 1 year	Review to see whether a further retention period is required
8.7	Visitors book			Current year + 2 years	Review to see whether a further retention period is required
8.8	PTA/Old Pupils Associations			Current year + 6 years	Review to see whether a further retention period is required

9.	Finance				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
9.1	Annual Accounts		Financial Regulations	Current year + 6 years	
9.2	Loans and grants		Financial Regulations	Date of last payment on loan + 12 years	Review to see whether a further retention period is required
9.3	Contracts				
9.3a	• under seal			Contract completion date + 12 years	SECURE DISPOSAL
9.3b	• under signature			Contract completion date + 6 years	SECURE DISPOSAL
9.3c	• monitoring records			Current year + 2 years	SECURE DISPOSAL
9.4	Copy orders			Current year + 2 years	SECURE DISPOSAL
9.5	Budget reports, budget monitoring etc.			Current year + 3 years	SECURE DISPOSAL

9.	Finance				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
9.6	Invoice, receipts and other records covered by the Financial Regulations		Financial Regulations	Current year + 6 years	SECURE DISPOSAL
9.7	Annual Budget and background papers			Current year + 6 years	SECURE DISPOSAL
9.8	Order books and requisitions			Current year + 6 years	SECURE DISPOSAL
9.9	Delivery Documentation			Current year + 6 years	SECURE DISPOSAL
9.10	Debtors' Records		Limitation Act 1980	Current year + 6 years	SECURE DISPOSAL
9.11	School Fund - Cheque books			Current year + 3 years	SECURE DISPOSAL
9.12	School Fund - Paying in books			Current year + 6 years then review	SECURE DISPOSAL
9.13	School Fund - Ledger			Current year + 6 years then review	SECURE DISPOSAL
9.14	School Fund - Invoices			Current year + 6 years then review	SECURE DISPOSAL
9.15	School Fund - Receipts			Current year + 6 years	SECURE DISPOSAL
9.16	School Fund - Bank statements			Current year + 6 years then review	SECURE DISPOSAL
9.17	School Fund - School Journey books			Current year + 6 years then review	SECURE DISPOSAL
9.18	Student grant applications			Current year + 3 years	SECURE DISPOSAL
9.19	Free school meals registers	Yes		Current year + 6 years	SECURE DISPOSAL
9.20	Petty cash books			Current year + 6 years	SECURE DISPOSAL

10.	Property				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
10.1	Title Deeds			Permanent	Permanent, these should follow the property unless the property has been registered at the Land Registry
10.2	Plans			Permanent	Retain in school whilst operational
10.3	Maintenance and contractors		Financial Regulations	Current year + 6 years	SECURE DISPOSAL
10.4	Leases			Expiry of lease + 6 years	SECURE DISPOSAL
10.5	Lettings			Current year + 3 years	SECURE DISPOSAL
10.6	Burglary, theft and vandalism report forms			Current year + 6 years	SECURE DISPOSAL
10.7	Maintenance log books			Current year + 6 years	SECURE DISPOSAL
10.8	Contractors' Reports			Current year + 6 years	SECURE DISPOSAL

11.	Local Authority				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
11.1	Secondary transfer sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
11.2	Attendance returns	Yes		Current year + 1 year	SECURE DISPOSAL
11.3	Circulars from LEA			Whilst required operationally	Review to see whether a further retention period is required

12.	Department for Children, Schools and Families				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
12.1	HMI reports			These do not need to be kept any longer	
12.2	OFSTED reports and papers			Replace former report with any new inspection report	Review to see whether a further retention period is required
12.3	Returns			Current year + 6 years	SECURE DISPOSAL
12.4	Circulars from Department for Children, Schools and Families			Whilst operationally required	Review to see whether a further retention period is required

13.	Connexions				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
13.1	Service level agreements			Until superseded	SECURE DISPOSAL
13.2	Work Experience agreement			DOB of child + 18 years	SECURE DISPOSAL

14.	Schools Meals				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
14.1	Dinner Register			Current year + 3 years	SECURE DISPOSAL
14.2	School Meals Summary Sheets			Current year + 3 years	SECURE DISPOSAL

15.	Family Liaison Officers and Home School Liaison Assistants				
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
15.1	Day Books	Yes		Current year + 2 years then review	SECURE DISPOSAL
15.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		Whilst the child is attending the school then destroy	SECURE DISPOSAL
15.3	Referral forms	Yes		While the referral is current	SECURE DISPOSAL
15.4	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	SECURE DISPOSAL
15.5	Contact database entries	Yes		Current year then review, if contact is no longer active then destroy	DELETE
15.6	Group Registers	Yes		Current year + 2 years	SECURE DISPOSAL

Annex R: Definition of Terms

Biometric Data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images;

Consent of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems or other media such as CCTV;

Data Subjects for the purpose of this policy include all living individuals about whom we hold personal data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their personal data.

Data Controllers means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Users include employees, volunteers, governors whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times;

Data Processors means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller;

Parent has the meaning given in the Education Act 1996 and includes any person having parental responsibility or care of a child;

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

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Privacy by Design means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR;

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Sensitive Personal Data means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

ANNEX S: FURTHER HELP AND SUPPORT AND RELEVANT LEGISLATION

For more information visit the website of the Information Commissioner's Office https://ico.org.uk/

Advice on online safety - http://www.thegrid.org.uk/eservices/safety/index.shtml

Further guidance - http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

School's toolkit is available - Record Management Society website
http://www.rms-gb.org.uk/resources/848

Test your online safety skills https://www.getsafeonline.org/

Data Protection Team - Email: - data.protection@hertfordshire.gov.uk

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication.

The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other acts relating to Online Safety

Racial and Religious Hatred Act 2006

It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with who they are in a position of trust. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

Communications Act 2003 (section 127)

Sending by means of the internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (Sections 1 - 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- Access to computer files or software without permission (for example using another person's password to access files).
- Unauthorized access, as above, in order to commit a further criminal act (such as fraud).
- Impair the operation of a computer or program.

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (Section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes.

It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (Sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child, for these purposes, is anyone under the age of 18.

Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

The Freedom of Information Act 2000

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

Counter-Terrorism and Security Act 2015 (Prevent), Anti-Radicalisation & Counter Extremism Guidance

https://www.gov.uk/government/publications/preventing-extremism-in-schools-andchildrens-services

ANNEX T: TECHNICAL ISSUES

Computer Viruses

- All files downloaded from the internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school ICT equipment.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through the ICT network office.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the network office who will advise you what actions to take and be responsible for advising others that need to know.

Infrastructure Monitoring and Security

St George's School has a monitoring solution via our internet service provider (SWITCHSHOP) where web-based activity is monitored and recorded.

School internet access is controlled through the Switchshop web-filtering and firewall service using enterprise level solution from FORTINET.

St George's School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; The General Data Protection Requirement 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

Staff and pupils are to be aware that school-based email and internet activity can be monitored and explored further if required.

The school does not allow pupils access to internet logs.

The school uses management control tools for controlling and monitoring workstations.

If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.

It is the responsibility of the school, by delegation to the Network Manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.

Pupils and staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility or the Network Manager's, to install or maintain virus protection on personal systems.

Pupils and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the ICT network office.

The ICT network office must be informed about any issues relating to viruses/anti-virus software.

Server Secure Practice

- Always keep servers in a locked and secure environment.
- Limit access rights.

- Always password protect and lock the server.
- Existing servers should have security software installed appropriate to the machine's specification.
- Back-up tapes should be encrypted by appropriate software.
- Data must be backed up regularly.
- Back-up tapes/discs must be securely stored.
- Back-up media stored off-site must be secure.
- Remote back-ups should be automatically securely encrypted. SITSS provide an encrypted remote back up service. Please contact the SITSS helpdesk for further information – 01438 844777.

Zombie Accounts

Zombie accounts refer to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such zombie accounts, when left active, can cause a security threat by allowing unauthorised access.

It is the job of the ICT network office to ensure that all user accounts are disabled once the member of the school has left.

User ID and passwords for staff and pupils who have left the school are removed from the system within **10 working days of Personnel telling the ICT network office a colleague has left.**

ANNEX U: DISPOSAL OF REDUNDANT ICT EQUIPMENT PROCEDURE

All redundant ICT equipment will be disposed of through an authorized agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant ICT equipment that may have held personal data will have the storage media over-written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed, it will be physically destroyed. We will only use authorized companies who will supply a written guarantee that this will happen.

Disposal of any ICT equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007 http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Data Protection Act 1998
https://ico.org.uk/for-organisations/education/

Electricity at Work Regulations 1989
http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.

The school's disposal record will include:

- Date item disposed of.
- Authorization for disposal, including verification of software licensing.
- How it was disposed of e.g. waste, gift, sale.
- Name of person &/or organisation who received the disposed item.

Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site:
http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

The Waste Electrical and Electronic Equipment Regulations 2006
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

ANNEX V: DEALING WITH SUBJECT ACCESS REQUESTS

The GDPR extends to all Data Subjects a right of access to their own personal data. A formal request from a Data Subject for information that we hold about them must be made in writing.

It is important that all members of staff are able to recognise that a written request made by a person for their own information may essentially be a Subject Access Request, even if the Data Subject does not specifically use this phrase in their request or refer to the GDPR. In some cases, a Data Subject may mistakenly refer to the "Freedom of Information Act" but this should not prevent the school from responding to the request as being made under the GDPR, if appropriate. Some requests may contain a combination of a Subject Access Request for personal data under the GDPR and a request for information under the Freedom of Information Act 2000 ("FOIA"). Requests for information under the FOIA must be dealt with promptly and in any event within 20 school days.

Any member of staff who receives a written request of this nature must immediately forward it to the DPO as the statutory time limit for responding is **one calendar month**.

In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. The school may ask the Data Subject for reasonable identification so that they can satisfy themselves about the person's identity before disclosing the information.

Requests from pupils who are considered mature enough to understand their rights under the GDPR will be processed as a subject access request as outlined below and the data will be given directly to the pupil (subject to any exemptions that apply under the GDPR or other legislation) [As the age when a young person is deemed to be able to give consent for online services is 13, we will use this age as a guide for when pupils may be considered mature enough to exercise their own subject access rights]. In every case it will be for the school, as Data Controller, to assess whether the child is capable of understanding their rights under the GDPR and the implications of their actions, and so decide whether the parent needs to make the request on the child's behalf. A parent would normally be expected to make a request on a child's behalf if the child is younger than 13 years of age.

Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.

Requests from parents in respect of their own child will be processed as requests made on behalf of the Data Subject (the child) where the pupil is aged under 13 (subject to any exemptions that apply under the Act or other legislation). If the parent makes a request for their child's personal data and the child is aged 13 or older and / or the school considers the child to be mature enough to understand their rights under the GDPR, the school shall ask the pupil for their consent to disclosure of the personal data if there is no other lawful basis for sharing the personal data with the parent (subject to any enactment or guidance which permits the school to disclose the personal data to a parent without the child's consent). If consent is not given to disclosure, the school shall not disclose the personal data if to do so would breach any of the data protection principles.

It should be noted that the Education (Pupil Information) (England) Regulations 2005 (the 'Regulations') applies to maintained schools so the rights available to parents in those regulations to access their child's educational records apply to the school. This means that following receipt of a request from a parent for a copy of their child's educational records, the school must provide a copy within 15 school days, subject to any exemptions or court orders which may apply.

The school may charge a fee for providing a copy of the educational record, depending on the number of pages as set out in the regulations. This is a separate statutory right that parents of children who attend maintained schools have so such requests should not be treated as a subject access request.

Where requests are "manifestly unfounded or excessive", in particular because they are repetitive, the school can:

- charge a reasonable fee taking into account the administrative costs of providing the information; or

- refuse to respond.

Where we refuse to respond to a request, the response will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Certain information may be exempt from disclosure so members of staff will need to consider what exemptions (if any) apply and decide whether you can rely on them. For example, information about third parties may be exempt from disclosure. In practice, this means that the school may be entitled or even required to withhold some documents entirely or will need to redact parts of them. Care should be taken to ensure that documents are redacted properly. The DPO will manage all subject access requests.

ANNEX W: Authorised Disclosures

The school will only disclose data about individuals if one of the lawful bases applies.

The school will regularly share personal data with third parties where it is lawful and appropriate to do so including, but not limited to, the following:

- Local Authorities
- the Department for Education
- the Disclosure and Barring Service
- the Teaching Regulation Agency
- the Teachers' Pension Service
- the Local Government Pension Scheme
- our external HR provider
- our external payroll provider
- our external IT provider
- HMRC
- the police or other law enforcement agencies
- our legal advisors and other consultants
- insurance providers
- occupational health advisors
- exam boards
- the Joint Council for Qualifications;
- NHS health professionals including educational psychologists and school nurses
- Education Welfare Officers
- Courts, if ordered to do so
- Prevent teams in accordance with the Prevent Duty on schools
- other schools, for example, if we are negotiating a managed move and we have consent to share information in these circumstances
- confidential waste collection companies

Some of the organisations we share personal data with may also be Data Controllers in their own right in which case we will be jointly controllers of personal data and may be jointly liable in the event of any data breaches.

The GDPR requires Data Controllers to have a written contract in place with Data Processors which must include specific clauses relating to the way in which the data is processed ('GDPR clauses'). Personal data may only be transferred to a third-party Data Processor if they agree to put in place adequate technical, organisational and security measures themselves.