ST DAVID'S
PREPARATORY SCHOOL

E-SAFETY POLICY

This policy covers all pupils including the Early Years Foundation Stage (EYFS)

INTRODUCTION AND OVERVIEW

The aim of this policy is to ensure a whole school approach to E-Safety. It applies to all members of the St David's Community (including staff, governors, students/ pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of St David's.

Rationale and Scope of the Policy

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at St David's School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of St David's School.
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

1. Content:

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), information about illegal substances.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites/radicalisation/terrorism sites and reports.
- Content validation: how to check authenticity and accuracy of online content.

2. Contact:

- Grooming
- Cyber-bullying in all forms.
- Identity theft and sharing passwords.

3. Conduct:

- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and well-being (amount of time spent online, either on the Internet or gaming).
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images).
- Copyright (little care or consideration for intellectual property and ownership – such as music and film) (Ref Ofsted 2013)

The Education and Inspections Act 2006 empowers the Head Teacher to regulate the behaviour of pupils when they are off site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching of electronic

devices and the deletion of data. St David's will deal with such incidents according to the Positive Behaviour and Anti-Bullying Policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

Role	Key Responsibilities
Head Teacher	• To take overall responsibility for e-safety provision. • As Senior Information Risk Owner (SIRO), to take overall responsibility for data, data security and General Data Protection Regulation (GDPR). • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements. • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant. • To be aware of procedures to be followed in the event of a serious e-safety incident. • To receive regular monitoring reports from the E-Safety Leader. • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager).

E-Safety Leaders	• To take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies/documents.
	• To promote an awareness and commitment to e-safeguarding throughout the school community.
	• To ensure that e-safety education is embedded across the curriculum
	• To liaise with school ICT technical/support staff.
	• To communicate regularly with SLT to discuss current issues, review incident logs and filtering and to change control logs.
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident.
	• To ensure that an e-safety incident log is kept up to date.
	• To facilitate training and advice for all staff.
	• To liaise with the Local Authority and relevant agencies.
	• To be regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • Sharing of personal data
	  • Access to illegal/inappropriate materials
	  • Inappropriate on-line contact with adults/strangers
	  • Potential or actual incidents of grooming
	  • Cyber-bullying and use of social media
	• To oversee the delivery of the e-safety element of the Computing curriculum.

Network Manager/ technician Currently Sweethaven Computers	• To report any e-safety related issues that arise to the E-Safety Leader. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy. • To ensure that provision exists for misuse detection and malicious attack (e.g. keeping virus protection up to date). • To regularly review the security of the school ICT system. • To ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices. • To ensure the school's procedure on web filtering is applied and updated on a regular basis. • To keep up to date with the school's E-Safety Policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant. • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures.
Governors	• To ensure that the school follows all current e-safety advice to keep the children and staff safe. • To approve the E-Safety Policy and review the effectiveness of the policy. • To receive regular information about e-safety incidents and monitoring reports. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities.

Role	Key Responsibilities
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities. • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant). • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff	• To read, understand and help promote the school's e-safety policies and guidance. • To read, understand, sign and adhere to the school Staff - Computing and ICT-Acceptable Use Policy. • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and to monitor their use and implement current school policies with regard to these devices. • To report any suspected misuse or problem to the E-Safety Leader or Head Teacher. • To maintain an awareness of current e-safety issues and guidance e.g. through CPD. • To model safe, responsible and professional behaviours in their own use of technology. • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• To read, understand, sign and adhere to the Pupil 'Computing and ICT - Acceptable Use Policy' (NB: at KS1 it would be expected that parents/carers would sign on behalf of the pupils). • To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • To understand the importance of reporting abuse, misuse or access to inappropriate materials and to know how to do so. • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To understand the importance of misuse or access to inappropriate materials and to be aware of the consequences. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking/use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school. • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home. • To help the school in the creation/review of e-safety policies.
Parents/carers	• To support the school in promoting e-safety by signing the 'Use of photographic Images Consent Form' which explains the school's use of photographic and video images. • To read, understand and promote the school Pupil Acceptable Use Agreement with their children. • To know and understand what the 'rules of appropriate use' are for pupils and what sanctions result from misuse by pupils. • To consult with the school if they have any concerns about their children's use of technology.
External groups	• Any external individual/organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school.

Communication of the Policy

The policy will be communicated to staff/pupils/community in the following ways:

- The policy is posted on the school website and is available in the staffroom and on Staffshare.
- The policy is part of school induction pack for new staff.
- The Acceptable use agreements are discussed with pupils at the start of each year.

- The Acceptable use agreements are issued to whole school community, usually on entry to the school.
- The Acceptable use agreements are held in pupil and personnel files.

Handling complaints

The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Discussion with Head Teacher and Computing & ICT Leader (if appropriate)
- Informing parents or carers
- Removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system.
- Referral to Local Authority/Police

The E-Safety Leader acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head Teacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy (see section below). Complaints related to child protection are dealt with in accordance with school/Local Authority child protection procedures (see Child Protection and Safeguarding policy)

Review and Monitoring

The E-Safety Policy is referenced from within other school policies and details can be found at the end of this policy.

- The school has an E-Safety Leader who will be responsible for document ownership, review and updates.
- The E-Safety Policy is reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- The E-Safety Policy has been written by the school E-Safety Leader and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school E-Safety Policy will be discussed in detail with all members of teaching staff.

EDUCATION AND CURRICULUM

Pupil E-safety Curriculum

This school has a clear, progressive e-safety education programme as part of the Computing curriculum as well as our Relationships and Health Education (RHE) and Personal, Social, Health and Economic Education (PSHE) curricula. Our lessons are built on the local authority e-safeguarding and e-literacy framework for EYFS to Y6, national guidance and other published schemes, for example the Jigsaw scheme of work. These lessons cover a range of skills and behaviours appropriate to their age and experience, including teaching children:

- To STOP and THINK before they CLICK.
- To develop a range of strategies to evaluate and verify information before accepting its accuracy.
- To be aware that the author of a web site/page may have a particular bias or purpose and to develop skills to recognise what that may be.
- To know how to narrow down or refine a search.
- [For older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings.
- To understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments.

- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
- To understand why they must not post pictures or videos of others without their permission.
- To know not to download any files – such as music files - without permission.
- To have strategies for dealing with receipt of inappropriate materials.
- [For older pupils] to understand why and how some people will 'groom' young people for sexual reasons.
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To understand that some people use the internet and social media to groom and radicalise other people especially children, young people and vulnerable adults and how to seek help if they feel they are affected by this.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

Teachers deliver the curriculum effectively by:

- Planning Internet use carefully to ensure that it is age-appropriate and supporting the learning objectives for specific curriculum areas.
- Reminding students about their responsibilities through an end-user Acceptable Use Policy which every student signs.
- Ensuring staff model safe and responsible behaviour in their own use of technology during lessons.
- Ensuring that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights.
- Ensuring that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include: risks in pop-ups; buying on-line; on-line gaming/ gambling and looking at loot box type issues.

Staff and Governor training

This school:

- Makes regular training available to staff on e-safety issues and the school's e-safety education programme, including being aware of the need to help children build their resilience to situations such as bullying, grooming, radicalisation and terrorism.
- Provides, as part of the induction process, all new staff (including those on university/college placement) with information and guidance on the E-Safety Policy and the school's Acceptable Use Policies.

Governors ensure that as part of the requirement for staff to undergo regularly updated safeguarding training and the requirement to ensure children are taught about safeguarding including on-line, that on-line safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

Parent awareness and training

This school runs a rolling programme of advice, guidance and training for parents, including:

- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safety behaviour are made clear.
- Information in school newsletters and on the school website giving suggestions for safe Internet use at home.
- Information meetings, visits by speakers, demonstrations and practical sessions held at school.
- Provision of information about national support sites for parents on the website.

Incident Management

In this school:

- There is strict monitoring and application of the E-Safety Policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions.
- All members and the wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.

- Support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues. We also have invaluable support in this area from our network administrators (currently Sweethaven Computers).
- Monitoring and reporting of e-safety incidents takes place and contributes to developments in policy and practice in e-safety within the school. Any records would be reviewed, audited and reported to the school's senior leaders, Governors and where necessary the LA and/or LSCB.
- Parents/carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

Cyberbullying

Please also refer to the Child Protection and Safeguarding Policy and Anti-Bullying Policy.

Cyberbullying has been defined in the following terms:
'Cyberbullying involves the use of information and communication technologies to support deliberate, repeated and hostile behaviour by an individual or group that is intended to harm others.'

Cyberbullying can involve Social Networking Sites (like Facebook, Twitter and Instagram etc.), emails and mobile phones used for SMS and other types of messaging and as cameras.

Cyberbullying can happen at all times of the day with a potentially bigger audience and more access as people forward on content at a click.

Cyberbullying – Preventative Measures

In addition to the preventative measures listed in this policy, St David's School:
- Blocks certain sites by its filtering system.
- May impose sanctions for the misuse, or attempted misuse of the internet.
- Offers guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe.
- Does not permit pupils to carry mobile phones in school (except Form 6 who may be travelling independently to and from school – see Computing, Mobile Device and Cameras Policy).
- Offers guidance to parents on online safety. This may be done formally, through parent workshops or informally through conversations or class talks.
- Encourages any parent or member of staff who has concerns about cyberbullying to report their concerns to the E-Safety Leader or a member of the SLT. This will then be investigated and, if appropriate, reported to parents and outside agencies.
- Allows all pupils to spend time in the Autumn term, either learning or revising the essentials of online safety. This is reinforced in Assembly time and PSHE lessons (particularly in the 'Celebrating Difference' and 'Relationships' units of the Jigsaw scheme of work) where pupils are encouraged to challenge what they see and read about on the internet and how to build up a resilience against the dangers and myths of online social media sites.
- Provide all staff with regular in-service training on cyberbullying.

MANAGING THE ICT INFRASTRUCTURE

Internet access, security (virus protection) and filtering

This school:
- Uses a combination of hardware and software security products to ensure age-appropriate content filtering is in place for Internet users at all times.
- Ensures network health through use of anti-malware and other security software.
- Blocks all Chat rooms and social networking sites.
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes.
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Ensures all staff and students have signed an acceptable use agreement form and understand that they must report any concerns.
- Ensures pupils only publish material within an appropriately secure environment.
- Requires staff to preview websites before use (where not previously viewed or cached), plan the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids. Google Safe Search is enforced for all users.

- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search.
- Informs all users that Internet use is monitored.
- Informs staff and students that that they must report any failure of the filtering systems directly to either the ICT & Computing Leader or directly to the system administrators.
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme.
- Provides advice and information on reporting offensive materials, abuse/bullying etc. available for pupils, staff and parents.
- Immediately refers any material we suspect is illegal to the appropriate authorities: Police and the Local Authority.
- Is currently working towards IASME and Cyber Essentials certification.

Network management (user access, backup)

This school:

- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services. Visiting music teachers and the PTA are the main users of this facility.
- Requires the Systems Administrator/network manager is up-to-date with school policies and statutory guidance.
- Ensures storage of all data within the school conforms to the UK data protection requirements.

To ensure the network is used safely, this school:

- Ensures new members of staff read and sign that they have understood the school's E-Safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to services is through a unique username and password. We also use the same username and password for access to our school's network.
- Ensures staff access to the school's management information system is controlled through a separate password for data security purposes.
- Provides pupils with an individual network log-in username (except Reception children) which gives them access to the school systems and the internet.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network and be a safeguarding risk.
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
- Requires all users to always log off when they have finished working or are leaving the computer unattended.
- Scans all mobile equipment with anti-virus/spyware before it is connected to the network.
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed. For example, projector filters cleaned by site manager/equipment installed and checked by approved suppliers/electrical engineers.
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role e.g. teachers access report writing module; Inclusion Leader - SEND data.
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school and system administrator software.
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems.
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data that complies with external Audit's requirements.
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network.
- Ensures our wireless network has been secured to industry standard Enterprise security level/ appropriate standards suitable for educational use.
- Ensures all computer equipment is installed professionally and meets health and safety standards.
- Ensures that large format displays are maintained so that the quality of presentation remains high.
- Reviews the school ICT systems regularly with regard to health and safety and security.

Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private and to change their password immediately and notify their Network Manager should they believe their password to be compromised.
- Staff are guided to use hard to guess passwords that are at least 12 characters long.
- Measures are in place to force regular password changes for staff.

E-mail

This school:

- Provides staff with an e-mail account for their professional use.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that e-mail systems are maintained and up to date.
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e-mails dangerous. We use a number of technologies to help protect users and systems in the school, including anti-malware software, , plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, Internet access is filtered by a hardware firewall device.

Staff are aware that:

- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to an external organisation must be written carefully (and may require authorisation), in the same way as a letter written on school headed paper.
- The sending of multiple or large attachments is limited, and may also be restricted by the provider of the service being used.
- The sending of chain letters is not permitted.

School website

The Head Teacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.

- Uploading of information is restricted to our website administrator.
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The point of contact on the website is the school address, telephone number and we use a general e-mail contact address (office@stdavidsschool.co.uk). Home information or individual e-mail identities will not be published.
- Photographs published on the web do not have full names attached.
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.
- We do not use embedded geodata in respect of stored images.
- We expect teachers using school approved blogs or wikis to password protect them and run them from the school website.

Social networking

Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the school's preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation. (See CCTV Policy)

DATA SECURITY: MANAGEMENT INFORMATION SYSTEM ACCESS AND DATA TRANSFER

Strategic and operational practices

At this school:

- We have taken the necessary steps to comply with Cyber Essentials and are in the process of applying for certification.
- We ensure staff know who to report incidents to where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record.
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
    - Staff
    - Governors
    - Pupils
    - Parents

  This makes clear staffs' responsibilities with regard to data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services/Family Services, Health, Welfare and Social Services.
- We require that any material must be encrypted if the material is to be removed from the school and that such data removal should be limited. We have an approved remote access solution so staff can access sensitive and other data from home, without the need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access must work within the approved system and follow the security processes required by those systems.
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have individual folders on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer.

EQUIPMENT AND DIGITAL CONTENT

For information about mobile phones, devices and taking images, please see the Computing, Mobile Device and Cameras Policy and the Taking, Storing and Using Images of Children Policy.

Digital images and video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/ personal equipment for taking pictures of pupils.
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use.
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

- The EYFS have two devices used for the Tapestry observation system. This system is securely protected and only the EYFS staff, the Head Teacher and parents have access to the data.

Asset disposal

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media professionally wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.

This policy is in compliance with the current version of 'Keeping Children Safe in Education' (DfE) and is linked to the following policies:

Anti-bullying
CCTV
Child Protection and Safeguarding
Computing - Acceptable Use Policies
Computing, Mobile Device and Cameras
ICT Network Management Policy
Personal, Social, Health and Economic Education
Positive Behaviour
Preventing Extremism and Anti Radicalisation
Relationships, Health & Sex Education
Staff Code of Conduct
Taking, Storing and Using Images of Children
Tapestry On-line Journal

Policy reviewed by E-Safety Leaders	F Izzard/C MacGregor	March 2023
Reviewed and approved by	SLT	April 2023
Reviewed and approved by	St David's Safeguarding Sub Committee	May 2023
Next Review (every year)		March 2024