VALLEY INVICTA
ACADEMIES TRUST

Online Safety Policy

Key document details

Policy number:	Policy type	Colleague responsible:	Date:	Next review:
TG14	Trust	Headteacher	September 2021	September 2022

Online Safety

The Trust believes that effective use of Information and Communications Technology (ICT) is essential in enhancing learning across the curriculum. Excellent use of ICT allows students to:

- Learn in a way that relates to their recreational culture;
- Utilise the power of multimedia and interactivity to learn and motivate;
- Gain access to a wide range of resources and research;
- Communicate easily with teachers, students and people outside the school environment;
- Present work in a professional manner;
- Develop innovation and problem-solving skills;
- Overcome some additional educational needs.

However, the Trust is fully aware that electronic technologies present a range of potential dangers for students and staff. As a result, this policy has been written to ensure that ICT is used effectively whilst minimising risk. Students, Staff, Governors and Trustees are advised, and expected, to take personal responsibility for their own use of electronic technologies.

All Stakeholders should be made aware of the dangers regarding sexting concerns and the process to be followed.

Writing and reviewing the Online Safety policy

The Online Safety Policy relates to other policies including those for ICT and for child protection. It encompasses the DfE statutory guidance 'Keeping Children Safe in Education' 2021, 'Early Years and Foundation Stage 2021', 'Working Together to Safeguard Children' 2018 and the local Kent Safeguarding Children Multi-Agency Partnership (KSCMP) procedures.

- Each school will appoint an appropriate member of staff to take responsibility for Online Safety, they will work with the school Designated Safeguarding Lead (DSL) as the roles overlap;
- Our Online Safety Policy has been written by the Trust, building on the Kent Online Safety Policy and government guidance. It has been agreed by senior management and approved by the Trust;
- The Online Safety Policy and its implementation will be reviewed annually;
- To ensure they have an oversight of online safety, the relevant Headteacher will be informed of online safety concerns, as appropriate.

The Online Safety Policy also makes use of, and reference to, the 'New Data Protection Act' (DPA) 2018 and the 'General Data Protection Regulation' (GDPR) 2018.

Teaching and Learning

Internet use will enhance learning

- The Trust Internet access will be designed expressly for student use and will include filtering appropriate to the age of students;
- Students will be taught the importance of personal responsibility in the safe and responsible use of the Internet;
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluations;
- The Trust aims to ensure equality of access for all.

Evaluating Internet content and copyright compliance

- The Trust should ensure that the use of Internet derived materials by staff, students, Governors and Trustees complies with copyright law and are appropriate to the learning needs of the students;
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Students and staff will be taught how to use the available Trust communication facilities including Learning Gateways and/or Virtual Learning Environments

- Appropriate members of the senior leadership team, and also those at middle management level (such as lead teachers), will monitor the usage of the Trust communication facilities. This is to include any Virtual Learning Environments (VLE) used by students and staff regularly in all areas, in particular message and communication tools and publishing facilities;
- Students, staff, Governors and Trustees will be advised on acceptable conduct and use when using the Trust communication facilities;
- Only members of the current student, parent/carer, staff, Governor and Trustees community will have access to the Trust communication facilities;
- All users will be mindful of copyright issues and will only upload appropriate content onto the Trust communication facilities.

Managing Internet access

Information system security

- School ICT systems capacity and security such as; firewalls, Internet traffic, blocked senders list and Internet filters will be reviewed on an on-going basis by the appropriate technical support teams;
- Virus protection will be installed and updated regularly;
- Security strategies will be implemented in line with the Local Authority and national guidelines.

Email

- Students may only use approved e-mail accounts on the school system. They will be provided e-mail accounts for educational use;
- Students should immediately tell a responsible adult if they receive an offensive e-mail;
- Students should not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission;
- School e-mail addresses and other official contact details should not be used for setting up personal social media accounts;
- E-mail should only be used for work/educational purposes; it should not be used for personal email;
- All e-mail messages should be sent using appropriate business like e-mail etiquette;
- E-mail sent to an external organisation should be written carefully and authorised by a teacher before sending;
- The forwarding of chain letters and the sending of offensive or inappropriate e-mails is not permitted and will result in a relevant behaviour sanction.

Published content and the school website

- The contact details on the website should be the school address, e-mail and telephone number;
- Staff, student, Governor and Trustee personal information will not be published;
- Staff, students, Governors and Trustees will take accountability/responsibility for materials posted on the web;
- Staff, student, Governors and Trustees need to be aware that publishing anything to the Internet at school or elsewhere which causes offence, or brings the school into disrepute, may lead to an exclusion or disciplinary action;
- Individual members of staff will take editorial responsibility and ensure that content is accurate and appropriate and conforms to the Trust Online Safety Policy.

Publishing students’ content including images, video and sound

- An overview will be kept by the appropriate member of the school’s leadership team of content published on the Trust websites and e-learning sites;
- A student’s work can only be published with the permission of the student and parents/carers;
- Photographs that include students will be selected carefully and will not enable the individual students to be clearly identified;
- Students’ full names will not be used anywhere on the website, blog, Twitter or any other social media used by the school particularly in association with photographs;
- Written permission from parents/carers will be obtained before photographs, video or sound of students are published on the Trust’s websites;
- Staff must seek guidance from the Online Safety Officer/IT Manager prior to allowing students to publish to external websites to ensure Online Safety and that Terms and Conditions are fully read and understood.

Social networking and personal publishing

- The Trust will block/filter access to social networking sites;
- The Trust will educate students in the responsible use of social networking and personal publishing on the web through ThinkuKnow or other appropriate training;
- Newsgroups will be blocked unless a specific use is approved;
- Students will be advised never to give out personal details of any kind which may identify them or their location;
- Students will be advised not to place personal photos, personal audio or personal videos on any social network space;
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications;
- Students should be encouraged to invite known friends only and deny access to others;
- Staff, students, Governors and Trustees will be advised on how to appropriately conduct themselves online. They will be informed of the potential risks and advised how to ensure that the settings on their accounts are set so as to keep themselves protected and to protect the reputation of the Trust.

Managing filtering

- The Trust will work in partnership with the Local Authority, Department for Education and the Internet Service Provider to ensure systems to protect students are reviewed and improved;
- If Staff, students, Governors or Trustees discover an unsuitable site, it must be reported to the appropriate member of staff or the Network Manager;
- The School Network Manager/IT Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing and/or webcams

- Internet Protocol (IP) videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet;
- Staff will ensure that external video-conferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure;
- Students should ask permission from the supervising teacher before making or answering a video-conference call;
- Video-conferencing will be appropriately supervised for the students’ ages;
- Cameras on devices should only be used after having been given permission to do so by a member of staff. They should only be used for educational purposes;
- All video-conferencing equipment will be switched off when not in use.

Managing emerging, mobile and smart technologies

- Emerging technologies will be examined for educational benefit and risk before use in school is allowed;
- Any data required and requested will be considered and evaluated before students are asked to use any new technologies;
- Mobile phones will not be used during lessons or formal school time unless it is of educational benefit and then only with supervision of a member of staff. The sending of abusive or inappropriate text messages is forbidden. Taking photographs and making phone calls using a mobile phone is also forbidden unless specific permission has been given;
- Staff will be issued with a school mobile phone where contact with students is required;
- Staff will be advised not to use personal or private mobile technologies/phones to contact students. It is strongly advised that staff do not text students from a personal mobile phone or mobile technology;
- If a student needs to contact their parents or carers while on site, they will be allowed to use a school phone and should not use their own personal device;
    - Parents are advised to contact their child via the school reception or appropriate administrator.
- If a student requires access to a personal device in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with the a relevant member of staff prior to use being permitted;
    - Any arrangements regarding access to personal devices in exceptional circumstances will be documented and recorded.
- Where students' mobile phones or personal devices are used when learning at home, this will be in accordance with our Acceptable Use Policy;
- Mobile phones and personal devices must not be taken into examinations. Students found in possession of a mobile phone or personal device which facilitates communication or internet access during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations;
- Any concerns regarding students' use of mobile technology or policy breaches will be dealt with in accordance with our existing policies, including anti-bullying, child protection and behaviour;
    - Staff may confiscate a student's mobile phone or device if they believe it is being used to contravene our child protection, behaviour or anti-bullying policy;
    - Searches of mobile phones or personal devices will be carried out in accordance with this policy and following advice given regarding this via the DfE: Searching, screening and confiscation (publishing.service.gov.uk);
    - The school is not required to inform parents before a search takes place or to seek their consent to search their child or their device;
    - Students' mobile phones or devices may be searched by a member of the Leadership Group, DSL or relevant member of the pastoral support team. Content may be deleted or requested to be deleted if it contravenes our policies;

- Mobile phones and devices that have been confiscated will be held in a secure place and released to the student at the end of the day, or if deemed appropriate, parent/carer upon arrangements being made;
- Appropriate sanctions and/or pastoral/welfare support will be implemented in line with our behaviour policy;
- Concerns regarding policy breaches by students will be shared with parents/carers as appropriate;
- Where there is a concern that a child is at risk of harm, we will contact the Local Authority Designated Officer (LADO); Kent Police; Education Safeguarding Team; Social Services – Children's Social Work Service;
- If there is suspicion that material on a student's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

Remote Learning and Communication

Leadership Oversight and Approval

- Remote learning will only take place using school approved systems;
  - ○ The identified system will have been assessed and approved by the Headteacher.
- Staff will only use school/VIAT managed professional accounts with learners and/or parents/carers;
  - ○ Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.
    - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the Designated Safeguarding Lead (DSL);
    - Staff will use work provided equipment where possible e.g. a school/VIAT laptop, tablet or other mobile device.
- Online contact with learners and/or parents/carers will not take place outside of the operating times as defined by SLT:
  - ○ Lesson times;
  - ○ Agreed meeting times with parents/carers which a more senior member of staff is made aware of;
  - ○ Arranged information or consultation events.
- All remote lessons will be formally timetabled; a Lead Teacher, member of SLG or DSL is able to drop in at any time;
- Live streamed remote learning sessions will only be held with approval and agreement from the Headteacher.

Data Protection and Security

- Any personal data used by staff and captured by system name when delivering remote learning will be processed and stored with appropriate consent and in accordance with our GDPR Privacy Notice:
  (https://www.invicta.viat.org.uk/download?file=https%3A%2F%2F0e58658be539ee7325a0-

220f04f871df648cf4a4d93a111e3366.ssl.cf3.rackcdn.com%2Finvicta_responsive%2Fuploads%2Fdocum ent%2FRAH-TG15-VIAT-GDPR-Privacy-Notice-Students-2020-2021.pdf%3Ft%3D1594808322);

- All remote learning and any other online communication will take place in line with current school/VIAT confidentiality expectations;
- All participants will be made aware that meetings/lessons are being recorded when this is taking place;
- Staff will not record lessons or meetings using personal equipment;
- Only members of current school/VIAT community will be given access to the remote learning system in use. Visitors may be invited to specific sessions if this is deemed to be professionally appropriate and/or educationally beneficial. A more senior member of staff should be consulted beforehand and made aware of this situation;
- Access to the school's remote learning system will be managed in line with current IT security expectations as outlined in this policy.

Session Management

- Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
    - Meeting IDs to be kept private and a password required to access these if possible;
    - Waiting rooms/lobbies used where available to manage entry to sessions;
    - Students asked to keep cameras off unless required for a specific purpose. If they are switched on, students should be wearing clothing in accordance with the school dress code policy.
- When live streaming with learners:
    - Contact will be made via learners' school/VIAT provided email accounts and/or logins;
    - Staff will mute/disable learners' videos and microphones unless specifically requested to enable these for educational/professional purposes;
    - At least 2 members of staff will have access to scheduled sessions.
- Live 1 to 1 sessions will only take place with approval from a member of SLG, DSL or direct line manager;
- A pre-agreed invitation detailing the session expectations will be sent to those invited to attend;
    - Access links should not be made public or shared by participants;
    - Learners and/or parents/carers should not forward or share access links;
    - Learners are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult. Behaviour during the session should comply with the school behaviour policy. Cameras and microphones should not be enabled unless a request for them to be enabled is made for educational and professional reasons only.
- Alternative approaches and/or access will be provided to those who do not have access.

Behaviour Expectations

- Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom;

- All participants are expected to behave in line with existing school/VIAT policies and expectations. This includes:
    - Appropriate language will be used by all attendees;
    - Staff will not take or record images for their own personal use;
    - Setting decisions about if other attendees can or cannot record events for their own use, and if so, any expectations or restrictions about onward sharing;
    - If sessions are recorded, all individuals involved should be informed;
    - If cameras are enabled, appropriate clothing will be worn, in line with school dress code policies and ideally students will engage in sessions in a communal/family space with at least one open door.
- Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session;
- When sharing videos and/or live streaming, participants are required to:
    - wear appropriate dress;
    - ensure backgrounds of videos are neutral (blurred if possible or an appropriate background added);
    - ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.
- Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches and Reporting Concerns

- Participants are encouraged to report concerns during remote and/or live streamed sessions to the DSL, or using the appropriate school specific recording systems (such as My Concern), as soon as possible;
- If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to an appropriate member of staff, such as Lead Teacher or Head of Year, and parents will be informed;
- Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour;
    - Sanctions for deliberate misuse will be in line with the appropriate school/Trust policies. These will include:
        - Behaviour Policy;
        - Online Safety Policy;
        - Anti-Bullying Policy).

Protecting personal data

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation, 2018:
    - Data Protection Policy;
    - VIAT GDPR Privacy Notice – for students;
    - VIAT GDPR Privacy Notice – for workforce;
    - VIAT Records Management Policy and Retention Guidelines.

  - All staff, students and visitors will be issued with user IDs and unique, complex passwords to the Trust's ICT systems;
  - Individuals should ensure that passwords are kept secure, changed on a frequent basis and include at least one capital, a combination of letters and numbers and a character or symbol such as @ or !;
  - All staff devices taken offsite should have a user account password or passcode enabled to stop unauthorised access to data on that device;
  - Staff need to lock, or log off and shut down completely, any school mobile devices being taken offsite;
  - They must ensure the password is enabled when the device is turned on;
  - Portable media is only allowed to be used with specific permission;
  - Any personal data sent over the internet must be encrypted.

Visitors' access to the School Network

- Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's Acceptable Use Agreement (AUA) and other associated policies, such as Anti-Bullying, Behaviour and Safeguarding.
- These devices should also all be used in line with the photographic procedures documented later in this policy.
- Approved visitors wishing to use the school's ICT facilities will be asked to sign a Visitor AUA and permitted a Visitor username and password providing access to the school's ICT facilities.
- Approved visitors, only wishing to access the school's Internet, will also be asked to sign a Visitor AUA and be provided with a Guest Wi-Fi code which will enable them access to the Internet until 4pm the same day.
- Guest Wi-Fi codes will be changed on a daily basis.

Policy decisions

Authorising Internet access

- All staff must read and fully understand the implications of the 'Staff Acceptable Use Agreement' before using any school ICT resource.
- The Trust will keep a record of all staff and students who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a student's access be withdrawn.
- Students and their parents/carers must apply for Internet access individually by signing and agreeing to comply with the school ICT Acceptable Use Agreement.
- The ICT AUA must include the wording:
- The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it is believed unauthorised use of the school's information systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
- Staff, students, Governors and Trustees should also be aware that the use of ICT should be

- consistent with the Trust ethos, other appropriate policies and the law.

Assessing risks

- The Trust will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The Trust cannot accept liability for the material accessed, or any consequences of Internet access.
- SECURUS, where installed, will be used to monitor staff and student access to unauthorised sites.
- When onsite all devices will make use of Lightspeed filtering and appropriate Mobile Device Management solutions will be put in place to monitor their use. Student devices provided via the eLearning scheme will also have this monitoring in place when offsite.
- The Trust should audit ICT provision to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.

Handling Online Safety complaints

- Complaints of Internet misuse will be dealt with by the appropriate member of staff, in the first instance.
- Any complaint about staff misuse must be referred to the Headteacher.
- Any complaint about Governor or Trustee misuse must be referred to the Chair of the relevant Board.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and will be referred to the DSL.
- Students, parents/carers will be informed of the complaints procedure and the procedure for reporting Online Safety concerns (such as breaches of filtering, cyberbullying, illegal content, sexting etc.).
- Where a potential illegal issue arises (such as breaches of filtering, cyberbullying, illegal content, sexting etc.) contact should be made with the Online Safety Officer and DSL who will then contact the following: Kent Police; Education Safeguarding Team; Social Services – Children’s Social Work Service to establish procedures for handling potentially illegal issues.
- Illegal images/materials located on any device including mobile phones should NOT be downloaded, sent to another user, printed or moved to another storage device unless this has been requested by the Police.
- In the case of illegal images, the device (mobile phone, netbook, laptop) should be confiscated at the Headteacher’s request and secured. The following will then also be contacted; Local Authority Designated Officer (LADO); Kent Police; Education Safeguarding Team; Social Services – Children’s Social Work Service.
- The SECURUS server, where installed, needs to be secured if indecent images are found by SECURUS on a student’s netbook, laptop or similar device.
- In the case of an illegal image being shared across the network, the network needs to be immediately blocked to users and the image isolated.

- The Head of Year will record incidents and actions taken using the appropriate year group recording method and also record in any other appropriate log e.g. Bullying or Child Protection log.
- The Online Safety Officer will also keep a central record of any incidents that occur.
- The DSL will be informed of any Online Safety incidents involving Child Protection concerns, which will then be escalated appropriately. The school will manage Online Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern, or fear that illegal activity has taken place or is taking place, then the school will contact the Children's Safeguarding Team or appropriate member of staff in school and escalate the concern to the Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County Council's Education Safeguarding Adviser (Online Protection).
- If an incident of concern needs to be passed beyond the school, then the concern will be escalated to the appropriate member of staff in school to communicate to other schools in Kent.
- If the school is made aware of an incident involving the creation and distribution of youth produced sexual imagery, such as "sexting", the school will act on accordance with advice given by the County Online Safety Officer and in-line with relevant Kent Safeguarding Child Board's procedures.

Communications policy

Introducing the Online Safety policy to students

- Expectations for Internet access will be posted in all networked rooms.
- Students will be informed that Internet use will be monitored.
- Students will have the Online Safety policy introduced to them during appropriately identified lessons in the initial weeks of Year 7. The lessons could be PSHEE, Computer Science or any other appropriate subject.
- Tutor time periods, Computer Science and PSHEE lessons will be used to revisit aspects of Online Safety. This will also be consolidated in any other lesson when and where links to appropriate behaviour can be made.

Staff and the Online Safety policy

- All staff will be given the School Online Safety policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues (as outlined above).

- Where an issue arises it should be reported to the line manager, the Online Safety Officer and the DSL.

Enlisting parents' support

- Parents'/carers' attention will be drawn to the School Online Safety Policy in newsletters, the school prospectus and on the Trust's websites.
- Information evenings will also be delivered and used as a vehicle to draw the attention of parents/carers to Online Safety and how they can help protect their children.

Photographic Images

Issues of consent

The 'New Data Protection Act' (DPA) 2018 and the 'General Data Protection Regulation' (GDPR) 2018 affect our use of photography. This is because an image of a child is personal data for the purpose of the Act, and it is a requirement that consent is obtained from the parent/carer of a child or young person under the age of 18 years for any photographs or video recordings for purposes beyond the school's core educational function (e.g. school websites, school productions). We recognise the importance of ascertaining the views of the child and these will be sought before images are used.

As it is likely that there will be a number of occasions during a student's school life when the school may wish to photograph or video that student, we will ensure that consent is sought when the student starts at the school, to last for the duration of their stay.

A signed consent form, as included in the Parent booklet will be obtained from the child's parent/carer, and kept on file, covering all cases where images of children are to be published beyond the parameters of school use.

Where the children are 'Looked After' the school must check consent on the corporate parent's behalf with the social worker and there may be other situations (in adoption placements or following a re-settlement from domestic violence for example), where a child's security is known by the class teacher to be at risk, indicating the need for extra care.

Parents/carers retain the right to withdraw consent at any stage, but they need to do so in writing.

Planning photographs of children

Images and details of students published together allow for the remote possibility that people outside the school could identify and then attempt to contact students directly. The measures described below should help to minimise the risk of such unsolicited attention.

- Where possible, photos will be general shots of classrooms or group activities rather than close up pictures of individual children. We will consider the camera angle; photographs taken over the shoulder, or from behind are less identifiable. However, images of students will not be published with the students' full names and appropriate close up pictures may be taken for internal, as well as external use and publicity.

- Images of students that will be used will include the students in suitable dress and there will be additional care taken if photographs of PE or swimming events are being taken.
- If children can be identified by logos or emblems on sweatshirts etc. the communications team will consider where the photograph is used. Where appropriate, alternatives to using the photograph will be considered.

Identifying students

The DfE advise the following, where consent is unclear, and we follow this advice:

- If the full name of the student is used, avoid using their photograph. If the photograph is used, avoid using the student's full name.

Using photographs of children supplied by a third party

Copyright does not apply to images for private family use. However, copyright does exist in commercial photographs and it rests with the photographer. Copyright is a right that the photographer automatically enjoys as the creator of the work to prevent other people exploiting his or her work and to control how other people use it.

Before using a photograph supplied by a third party it must be checked to ensure that the third party owns the copyright in the photograph and their written or verbally recorded permission to use it will be obtained. Photographs used without the copyright owner's permission, could result in an action being taken against the offending party for copyright infringement.

Images downloaded from the Internet are also subject to copyright.

School prospectus and other literature

Most school literature is aimed at a specific audience. However, we will endeavour to ensure that we avoid using personal details or full names of any child in a photograph.

Websites

This is an area that gives particular concern to parents/carers because of the potential misuse of images by paedophiles. With digital photography there is the remote possibility that images of children could be produced, manipulated, and circulated, without the parents'/carers' or children's knowledge. The dual concern which follows such a risk is that children might be exploited and a school might be criticised or face action.

It is important to take care with identification and to respect parental views on the use of any photography of children on a website.

Parental right to take photographs and videos

Parents/carers are not covered by the DPA, 2018 if they are taking photographs or making a video recording for their own private use. The Act does not, therefore, stop parents/carers from taking photographs or making video recordings at school events. The decision to not allow parents/carers and visitors to take photographs and videos is, therefore, made by the Headteacher and parents should be reminded of this policy being in place. This decision is made so as to protect the young people taking part in the different school events.

Parents/carers are absolutely not permitted to take photographs or to make a video recording for anything other than their own personal use. Recording and/or photographing other than for private use would require the consent of the other parents whose children may be captured on film. Without this consent the DPA, 2018, would be breached.

The storage of photographs and videos

Photographs and videos must be maintained securely for authorised school use only, and disposed of either by return to the child, parents/carers or shredding as appropriate.
If photographs and videos will be taken (i.e. on a school trip) using a school mobile phone or school camera, the images stored on them should be removed as soon as possible and stored on a secure school network location.
When staff use their own professional standard cameras, a school owned SD card must be used so that data is not stored on the personal device.
Under no circumstances should photographs and videos of students be stored on staff personal devices or storage media.

Open Events

The school may take photographs and video recordings at Open Events. At these events there will be clear signage informing visitors and guests that photographs and videos will be taken. The signage should also identify that these may be used for internal/external use and publicity. Should anyone wish to not be photographed or videoed they should make themselves known so that appropriate action can be taken to ensure that they are omitted from these.