E-SAFETY POLICY

Policy adopted by RISE Learning Zone: 01.09.2015
Last reviewed: September 2018
Next review: September 2020
Policy Document SP-21

Education and Curriculum

Pupil e-Safety curriculum
This provision

- *Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:*
    - *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 know how to report any abuse including cyberbullying; and how to 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.*

- *Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.*
- *Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the provision/will be displayed when a student logs on to the provision network.*
- *Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.*
- *Ensures 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;*

- *Ensures 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;*

Staff training
This provision

- *Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;*
- *Makes regular training available to staff on e-safety issues and the provision's e-safety education program.*
- *Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the eSafeguarding policy and the provision's Acceptable Use Policies.*

Parent awareness and training
This provision

- *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-safe behaviour are made clear*
    - *Information leaflets; in provision newsletters; on the provision web site;*
    - *demonstrations, practical sessions held at provision;*
    - *suggestions for safe Internet use at home;*
    - *provision of information about national support sites for parents.*

Expected Conduct and Incident management

Expected conduct

In this provision, all users:

- *are responsible for using the provision ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to provision systems. (at KS1 it would be expected that parents/carers would sign on behalf of the pupils.)*
- *need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences*
- *need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so*
- *should understand the importance of adopting good e-safety practice when using digital technologies out of provision and realise that the provision's E-Safety Policy covers their actions out of provision, if related to their membership of the provision*
- *will be expected to know and understand provision policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand provision policies on the taking / use of images and on cyber-bullying*

Staff

- *are responsible for reading the provision's e-safety policy and using the provision ICT systems accordingly, including the use of mobile phones, and hand held devices.*

Students/Pupils

- *should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations*

Parents/Carers

- *should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the provision*
- *should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse*

Incident Management

In this provision:

- *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 its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the provision's escalation processes.*
- *support is actively sought from other agencies as needed (eg the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues*
- *monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the provision. The records are reviewed/audited and reported to the provision's senior leaders, Governors /the LA / 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*

Managing the ICT infrastructure

- ***Internet access, security (virus protection) and filtering***

This provision:

- *Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;*
- *Uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;*
- *Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;*
- *Ensures network healthy through use of Sophos anti-virus software (from LGfL) etc and network set-up so staff and pupils cannot download executable files;*
- *Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;*
- *Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;*
- *Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;*
- *Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;*
- *Uses security time-outs on Internet access where practicable / useful;*
- *Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;*

- *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 understands that they must report any concerns;*
- *Ensures pupils only publish within an appropriately secure environment : the provision's learning environment.*
- *Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the provision's Learning Platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; eg yahoo for kids or ask for kids , Google Safe Search , ...*
- *Never allows / 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 the [system administrator / teacher / person responsible for URL filtering]. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL Helpdesk as necessary;*
- *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 LA.*

- ***Network management (user access, backup)***

This provision

- *Uses individual, audited log-ins for all users.*
- *Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services*
- *Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;*
- *Has additional local network auditing software installed;*
- *Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;*
- *Storage of all data within the provision will conform to the UK data protection requirements*

Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.
To ensure the network is used safely, this provision:

- *Ensures staff read and sign that they have understood the provision's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide a different / use the same username and password for access to our provision's network;*
- *Staff access to the provisions' management information system is controlled through a separate password for data security purposes;*
- *We provide pupils with an individual network log-in username. From Year X they are also expected to use a personal password;*
- *All pupils have their own unique username and password which gives them access to the Internet, the Learning Platform and (for older pupils) their own provision approved email account;*
- *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;*
- *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;*
- *Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.*
- *Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day.*
- *Has set-up the network so that users cannot download executable files / programmes;*
- *Has blocked access to music/media download or shopping sites – except those approved for educational purposes;*
- *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 provision 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 provision, is used solely to support their professional responsibilities and that they notify the provision of any "significant personal use" as defined by HM Revenue & Customs.*
- *Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc*
- *Maintains equipment to ensure Health and Safety is followed;*
  e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / LA 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; SEN coordinator - SEN data;
- *Ensures that access to the provision's network resources from remote locations by staff is restricted and access is only through provision / LA approved systems:*
  e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution / RAv3 system;
- *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; e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child;*
- *Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password (their USO username and password);*
- *Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;*
- *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;*
- *Uses our broadband network for our CCTV system and have had set-up by approved partners;*
- *Uses the DfE secure s2s website for all CTF files sent to other provisions;*
- *Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);*
- *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;*
- *Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;*
- *All computer equipment is installed professionally and meets health and safety standards;*
- *Projectors are maintained so that the quality of presentation remains high;*
- *Reviews the provision ICT systems regularly with regard to health and safety and security.*

Passwords policy

- *This provision 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. ;*
- *All staff have their own unique username and private passwords to access provision systems. Staff are responsible for keeping their password private.*

E-mail
This provision

- *Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account;*
- *Does not publish personal e-mail addresses of pupils or staff on the provision website. We use anonymous or group e-mail addresses.*

- *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 email accounts 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.*

Pupils:

- *Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work.*
- *Pupils are taught about the safety and 'netiquette' of using e-mail both in provision and at home i.e. they are taught:*
    - *not to give out their e-mail address unless it is part of a provision managed project or to someone they know and trust and is approved by their teacher or parent/carer;*
    - *that an e-mail is a form of publishing where the message should be clear, short and concise;*
    - *that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on provision headed paper;*
    - *they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;*
    - *to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;*
    - *that they should think carefully before sending any attachments;*
    - *embedding adverts is not allowed;*
    - *that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;*
    - *not to respond to malicious or threatening messages;*
    - *not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;*
    - *not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;*
    - *that forwarding 'chain' e-mail letters is not permitted.*

- *Pupils sign the provision Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.*

Staff:

- *Staff can only use the Zone e mail systems on the provision system*
- *Staff only use Zone e-mail systems for professional purposes*
- *Access in provision to external personal e mail accounts may be blocked*
- *Staff use a 'closed' Zone email system which is used for Zone communications and some 'Zone approved' transfers of information ;*
- *Never use email to transfer staff or pupil personal data. We use secure, Zone / DfE approved systems. These include: S2S (for provision to provision transfer); Collect; USO-FX, named Zone system;*
- *Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on provision headed paper. That it should follow the provision 'house-style':*
    - *the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;*
    - *the sending of chain letters is not permitted;*
    - *embedding adverts is not allowed;*

- *All staff sign our Zone / provision Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.*

Provision website

- *The Headteacher 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 authorisers.*
- *The provision web site complies with the statutory DfE guidelines for publications;*
- *Most material is the provision'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 web site is the provision address, telephone number and we use a general email contact address, e.g. info@provisionaddress or admin@provisionaddress. 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 provision website;*
- *We do not use embedded geodata in respect of stored images*
- *We expect teachers using' provision approved blogs or wikis to password protect them and run from the provision website.*

Learning platform

- *Uploading of information on the provisions' Learning Platform / virtual learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;*
- *Photographs and videos uploaded to the provisions Platform will only be accessible by members of the provision community;*
- *In provision, pupils are only able to upload and publish within provision approved and closed systems, such as the Learning Platform;*

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 provisions' preferred system for such communications.*
- *The provision's preferred system for social networking will be maintained in adherence with the communications policy.*

Provision staff will ensure that in private use:

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

Video Conferencing
This provision

- *Only uses the Zone supported services for video conferencing activity;*
- *Only uses approved or checked webcam sites;*

CCTV

- *We have CCTV in the provision 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.*
- *We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.*

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this provision:

- *The Head Teacher is the Senior Information Risk Officer (SIRO).*
- *Staff are clear who are the key contact(s) for key provision information (the Information Asset Owners) are.*
- *We ensure staff know who to report any incidents 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 provision 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 Zone 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 Protect and Restricted material must be encrypted if the material is to be removed from the provision and limit such data removal. / We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.*
- *Provision staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.*
- *We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.*

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- *Designated 'mobile use free' areas are situated in the setting, and signs to this effect are to be displayed throughout. The areas which should be considered most vulnerable include: toilets, bathrooms and in some settings - sleep areas and changing areas.*
- *Mobile phones brought into provision are entirely at the staff member, student's & parents' or visitors own risk. The Provision accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into provision.*
- *Student mobile phones which are brought into provision must be turned off (not placed on silent) and stored out of sight on arrival at provision. They must remain turned off and out of sight until the end of the day. Staff members may use their phones during provision break times.*
  All visitors are requested to keep their phones on silent.
- *The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.*
- *The Provision reserves the right to search the content of any mobile or handheld devices on the provision premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.*
- *Where parents or students need to contact each other during the provision day, they should do so only through the Provision's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the provision office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.*
- *Mobile phones and personally-owned devices will not be used in any way during lessons or formal provision time. They should be switched off or silent at all times.*
- *Mobile phones and personally-owned mobile devices brought in to provision are the responsibility of the device owner. The provision accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.*
- *Mobile phones and personally-owned devices are not permitted to be used in certain areas within the provision site, e.g. changing rooms and toilets.*
- *Mobile phones will not be used during lessons or formal provision time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.*
- *The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.*
- *Personal mobile phones will only be used during lessons with permission from the teacher.*
- *No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.*
- *All mobile phones and personally-owned devices will be handed in at reception should they be brought into provision.*

Students' use of personal devices

- *The Provision strongly advises that student mobile phones should not be brought into provision.*
- *The Provision accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.*
- *If a student breaches the provision policy then the phone or device will be confiscated and will be held in a secure place in the provision office. Mobile phones and devices will be released to parents or carers in accordance with the provision policy.*

- *Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.*
- *If a student needs to contact his or her parents or carers, they will be allowed to use a provision phone. Parents are advised not to contact their child via their mobile phone during the provision day, but to contact the provision office.*
- *Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.*
- *Students will be provided with provision mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.*
- *No students should bring his or her mobile phone or personally-owned device into provision. Any device brought into provision will be confiscated.*

Staff use of personal devices

- *Staff handheld devices, including mobile phones and personal cameras must be noted in provision – name, make & model, serial number. Any permitted images or files taken in provision must be downloaded from the device and deleted in provision before the end of the day.*
- *Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.*
- *Staff will be issued with a provision phone where contact with students, parents or carers is required.*
- *Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.*
- *If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.*
- *Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.*
- *If a member of staff breaches the provision policy then disciplinary action may be taken.*
- *Where staff members are required to use a mobile phone for provision duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a provision mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a provision-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.*

Digital images and video
In this provision:

- *We gain parental / carer permission for use of digital photographs or video involving their child as part of the provision agreement form when their daughter / son joins the provision;*
- *We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published provision produced video materials / DVDs;*
- *Staff sign the provision'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 provision web site, in the prospectus or in other high profile publications the provision will obtain individual parental or pupil permission for its long term use*
- *The provision 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 eSafety 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 identify of others and their location, such as house number, street name or provision. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.*