EAST MIDLANDS VOCATIONAL ACADEMY LIMITED

E-SAFETY POLICY

Contents

1. Introduction and Overview

Rationale
The purpose of this policy is to:

- set out the key principles expected of all members of the school community at East Midlands Vocational Academy Ltd with respect to the use of ICT-based technologies.;
- safeguard and protect the children and staff of East Midlands Vocational Academy Ltd;
- 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:
Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse;
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites;
- hate sites;
- content validation: how to check authenticity and accuracy of online content.

Contact

- grooming;
- cyber-bullying in all forms;
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords.

Conduct

- privacy issues, including disclosure of personal information;
- digital footprint and online reputation;
- health and well-being (amount of time spent online (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).

Scope
This policy applies to all members of East Midlands Vocational Academy Ltd (EMVA) (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school / academy ICT systems, both in and out of East Midlands Vocational Academy Ltd.

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

Role	Key Responsibilities

Directors	• To take overall responsibility for e-Safety provision.
	• To take overall responsibility for data and data security.
	• 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 ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures.
	• Liaises with school ICT technical staff.
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident.
	• facilitates training and advice for all staff.
	• Ensures that e-safety education is embedded across the curriculum.
	• To ensure that an e-Safety incident log is kept up to date.
	• liaises with the Local Authority and relevant agencies.
	• Is 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 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. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor.

Role	Key Responsibilities
All staff	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents. • Promotes an awareness and commitment to e-safeguarding. throughout the school community. • To support the school in encouraging parents and the wider. community to become engaged in e-safety activities. • To report any e-Safety related issues that arises, to the Managing Director. • To ensure that users may only access the school's networks. through an authorised and properly enforced password protection policy, in which passwords are regularly changed. • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date). • To ensure 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. • the school's policy on web filtering is applied and updated on a regular basis. • To ensure that all data held on pupils on the school office machines have appropriate access controls in place. • 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. • To read, understand and help promote the school's e-Safety policies and guidance. • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices. • To report any suspected misuse or problem to the e-Safety coordinator. • 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. • 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. • To know what action to take if they or someone they know feels worried or vulnerable when using online technology.

Role	Key Responsibilities
	• 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 and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images. • To consult with the school if they have any concerns about their children's use of technology.

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

- Policy to be posted on the school website and on EMVA premises;
- Policy to be part of school induction pack for new staff.

Handling complaints:

- EMVA 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. Neither the school nor the Local Authority can 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:
  - interview/counselling by tutor / Managing Director;
  - informing parents or carers;
  - removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
  - referral to LA / Police.
- The Managing Director acts as first point of contact for any complaint;
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring

- The Managing Director will be responsible for document ownership, review and updates;

- The e-safety policy will be 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 Managing Director and is current and appropriate for its intended audience and purpose.

2. Education and Curriculum

Pupil e-Safety curriculum

EMVA:

- E-safety training is given to staff and students in the form of discussions and training courses as available and includes:
    - 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 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;
- 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

EMVA:

- 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 school's e-safety education program; Monthly staff meetings;
- 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.

3. Expected Conduct and Incident management

Expected conduct

At EMVA, all users:

- Are responsible for using the school ICT systems correctly;
- 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 school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school;
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

Staff

- Are responsible for reading EMVA's e-safety policy and using the school 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 EMVA;
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Incident Management

At EMVA:

- 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 school'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 EMVA. The records are reviewed/audited and reported to the Managing Director;
- 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.

4. Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

EMVA:

- Has secure broadband connectivity only accessible to staff;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network;
- 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;
- 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;
- Informs all users that Internet use is monitored;
- 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)

EMVA:

- Uses individual, audited log-ins for all users;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Storage of all data within the school 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, EMVA:

- Ensures 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 service is through a unique, audited username and password. We also *provide a different / use the same username and password* for access to EMVA network;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- We provide pupils with an individual network log-in username;
- All pupils have their own unique username and password which gives them access to 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;
- 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;
- 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 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;
  e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / LA electrical engineers;
- 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;
- Uses our broadband network for our CCTV system and have had set-up by approved partners;
- Projectors are maintained so that the quality of presentation remains high;

- Reviews the school ICT systems regularly with regard to health and safety and security.

Passwords policy

- EMVA 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 school systems. Staff are responsible for keeping their password private;
- We require staff to use strong passwords;
- We require staff to change their passwords twice a year.

E-mail

EMVA:

- Provides staff with an email account for their professional use;
- Does not publish personal e-mail addresses of pupils or staff on the school website; We use anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk / head@schoolname.la.sch.uk / or class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public;
- 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 school and at home i.e. they are taught:
    - Not to give out their e-mail address unless it is part of a school 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 school 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.

Staff:

- Access in school to external personal e mail accounts may be blocked;
- Never use email to transfer staff or pupil personal data;
- 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 school headed paper. That it should follow the school '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.

School website

- The Managing Director 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 school web site complies with the statutory DfE guidelines for publications;
- 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 web site is the school address, telephone number and we use a general email contact address, e.g. info@schooladdress or admin@schooladdress. 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 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 schools' 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 EMVA or local authority;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing

EMVA:

- Only uses approved or checked webcam sites.

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.

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

Strategic and operational practices

EMVA:

- The Managing Director is the Senior Information Risk Officer (SIRO);
- 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;
- School staff with access to setting-up usernames and passwords for email, network 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.

Technical Solutions

- We store any Protect and Restricted written material in a lockable cabinet;
- We lock any back-up tapes in a secure, fire-proof cabinet or take the off site;
- Paper based sensitive information is shredded, using cross cut shredder.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, student's & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school;
- Student mobile phones which are brought into school must be turned given to tutors at the beginning of each lesson and locked in the staff office. They will be returned at 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 Managing Director. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Managing Director is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary;
- The School reserves the right to search the content of any mobile or handheld devices on the school 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 school day, they should do so only through the School'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 school 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 school time. They should be switched off or silent at all times;
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school 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 school site, e.g. changing rooms and toilets;
- Mobile phones will not be used during lessons or formal school 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 school.

Students' use of personal devices

- EMVA strongly advises that student mobile phones should not be brought into school;
- The School 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 school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school 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 school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school 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 school 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;

Staff use of personal devices

- Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school 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 school 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 the Managing Director 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 Managing Director;
- 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 school policy then disciplinary action may be taken;
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes;

Digital images and video

EMVA:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son 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;
- 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 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 school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.