Winnington Park Primary School and Nursery

Online Safety Policy

Completed by: Kay Ikin

Updated: Autumn 2023

Review date: Autumn 2024

Introduction and Aims

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Winnington Park Primary School and Nursery (WPPS&N) with respect to the safe use of IT-based technologies
- Safeguard and protect the children and staff of WPPS&N
- Have clear structures to deal with online abuse such as online bullying 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
- To meet Articles 13 and 17 for Rights of the child; this states every child has the right to express their thoughts and opinions and access all kinds of information. It also states that we must protect children from material that could harm them

This policy should also be read in conjunction with Acceptable Use of Communications Policy, Mobile Phone Policy, Safeguarding Children Policy, Anti-Bullying Policy and Guidance on the Use of Photographic Images and Videos of Children in Schools.

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

- 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
- Grooming
- Online bullying in all forms

- Identity theft, including 'frape' (hacking Facebook profiles) and sharing passwords
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, using the Internet or gaming)
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Extremism
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

Scope

This policy applies to all members of the WPPS&N community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of School's IT systems and devices both on and off site.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of Online bullying, or other Online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The School 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 online safety behaviour that take place out of school.

Roles and Responsibilities

Role	Key Responsibilities
Headteacher	• To take overall responsibility for Online Safety provision • To take overall responsibility for data and data security (SIRO) • 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 Online 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 Online safety procedures (e.g. network manager)
Designated Child Protection Leader	• Takes day to day responsibility for Online safety issues and has a leading role in establishing and reviewing the school Online safety policies / documents • Promotes an awareness and commitment to Online safeguarding throughout the school community • Ensures that Online safety education is embedded across the curriculum • Liaises with school technical staff • To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident • To ensure that an Online safety incident log is kept up to date (CPOMS) • Facilitates training and advice for all staff • Liaises with the Local Authority and relevant agencies

Role	Key Responsibilities
	• 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 • Online bullying and use of social media
Governors	• To ensure that the school follows all current Online safety advice to keep the children and staff safe • To approve and review the effectiveness of the Online Safety Policy and associated policies. This will be carried out by the Safeguarding or Curriculum Committee and ratified by Full Governors. Governors will receive regular information about online safety incidents and monitoring reports through the Headteacher's report • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the Online Safety Governor will include: • Regular review with the Online Safety Co-ordinator / Officer • Online safety incident logs, filtering / change control logs)
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum • To liaise with the online safety coordinator regularly (where this is not the Computing Leader)
Network Manager / Office Manager / Network Technician	• To report any online safety related issues that arise, to the Online safety coordinator

Role	Key Responsibilities
	• 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 IT 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 • CWAC is informed of issues relating to the filtering applied by the LA • That he / she keeps up to date with the school's Online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of the network / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster • To keep up-to-date documentation of the school's online security and technical procedures • To ensure that all data held on pupils on the school office machines have appropriate access controls in place

Role	Key Responsibilities
Teachers and Teaching Assistants	• To embed online safety issues in all aspects of the curriculum and other school activities • To plan and effectively deliver the School's On-line safety and Computing curriculum • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the school's on-line safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of online 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 online safety coordinator • To maintain an awareness of current online 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

Role	Key Responsibilities
Pupils	• Read, understand and agree to adhere to the Pupil Acceptable Use Policy • 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 • 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 online safety practice when using digital technologies out of school and realise that the school's Online 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 on-line safety policies
Parents/carers	• To support the school in promoting online 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 read, understand and promote the School's Pupil Acceptable Use Agreement with their children • To consult with the school if they have any concerns about their children's use of technology

Role	Key Responsibilities
External groups	• To follow all advice and guidance as provided by members of the school staff and to follow the guidance in the school Code of Conduct and School Handbook

Communication:

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

- Policy to be posted on the school website
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year
- Acceptable use agreements to be issued to all employees and permanently contracted staff, usually on entry to the school and then annually
- Acceptable use agreements to be held in personnel files

The school will take all reasonable precautions to ensure online 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 class teacher / Computing Subject Leader / Headteacher
    - informing parents or carers
    - removal of Internet or computer access for a period
    - referral to LA / Police

- Our Headteacher acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher

- Complaints of online bullying 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

Pupil Online Safety Curriculum

This school

- Has a clear, progressive On-line safety education programme as part of the Computing 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
- to understand the impact of online bullying, sexting, extremism 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 online bullying; 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

Staff and Governor Training

This school

- 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 online safety issues and the school's online safety education program through staff meetings
- Provides, as part of the induction process, all new staff with information and guidance on this policy, the school's Acceptable Use Policies and Mobile Phone Policy

Parent Awareness and Training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
  - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of online safe behaviour are made clear
  - Information leaflets; in school newsletters
  - On the school web site; ensure up to date information, web links and advice on how to keep their children safe on-line
  - Demonstrations, practical sessions held at school at least every 3 years.
  - Suggestions for Safe Internet use at home
  - Provision of information about national support sites for parents

Supporting Information

Expected Conduct

In this school, all users:

- Are responsible for using the school computing systems and internet linked devices in accordance with the relevant Acceptable Use Agreement and Acceptable use of Communications Policy
- 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 online safety practice when using digital technologies out of school and realise that the school's Online 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 online bullying

Staff

- Are responsible for reading the school's Online Safety policy and using the school Computing 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 know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

In this school:

- There is strict monitoring and application of the Online 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 (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with online safety issues
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in on-line safety within the school. The records are reviewed/audited and reported to the school's senior leaders and Governors
- Parents / carers are specifically informed of online 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. Also, with staff, if it is deemed necessary, the LADO will be contacted

Internet Access, Security (virus protection) and Filtering

This school:

- Uses the CWAC 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 LA approved systems for secured email to send personal data over the Internet and uses encrypted devices
- 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
- Works in partnership with the CWAC 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 understand the acceptable use agreement form and understand that they must report any concerns
- Ensures pupils only publish within an appropriately secure environment: the School's virtual learning environment
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school'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; e.g. 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 / School's virtual learning environment is monitored
- Informs staff and students that that they must report any failure of the filtering systems directly to the Headteacher, network technician or Computing Subject Leader. Our system administrator(s) logs or escalates as appropriate to the Technical service provider 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 school

- 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, this school:

- Ensures staff read and sign that they have understood the school's Online 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 school's 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. From Year 1 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 and Purple Mash
- 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 and put laptops and internet linked devices into locked cupboards and draws
- 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
- 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 school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems
- 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

- 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
- 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 the DfE secure s2s website for all CTF files sent to other schools
- 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
- 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 school IT systems regularly with regard to health and safety and security

Passwords

See the guidance and requirements in the Acceptable Use of Communications Policy

E-mail

This school

- Provides staff with an email account for their professional use: Microsoft 365
- Does not publish personal e-mail addresses of pupils or staff on the school website

- 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 Computing scheme of work
- Pupils can only receive external mail from, and send external mail to, addresses if the SafeMail rules have been set to allow this
- Pupils are taught about the online 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

- Pupils sign the school 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 Google (gmail) e-mail on the school system following guidance within the Acceptable Use of Communications Policy
- Access in school to external personal e mail accounts may be blocked
- 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.
    - 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 Acceptable Use Agreement 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

School Website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- 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 admin@winningtonpark.cheshire.sch.uk Home information or individual e-mail identities will not be published
- Photographs published on the web do not have full names attached
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website
- We do not use embedded geodata in respect of stored images
- We expect teachers using' school approved blogs or wikis to password protect them and run 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.

  School staff will ensure that in private use they adhere to the guidance in the Acceptable Use of Communications Policy. In summary:

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

Strategic and Operational Practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO) and is supported by the school's Bursar

- Staff are clear who are the key contact(s) for key school 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: paper copies are held in the school office
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed
    - staff
    - governors
    - pupils (do not sign but are made familiar with the policy each term and the principles of on-line safety and acceptable use through the curriculum)
    - parents

  This makes clear staffs' responsibilities with regard to data security, passwords and access
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services
- We require that any Protect and Restricted material must be encrypted (all memory sticks are to be encrypted) if the material is to be removed from the school 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
- School 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 undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored

Technical Solutions

- Staff have personal data space on the staff server to store sensitive documents or photographs that can only be accessed by themselves

- We require staff to log-out of systems when leaving their computer
- We use encrypted flash drives if any member of staff has to take any sensitive information off site
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools
- We use CWAC approved systems to transfer other data to schools, such as references, reports of children
- We store any Protect and Restricted written material in lockable storage units
- All servers are managed by DBS-checked staff
- We use remote secure back-up for disaster recovery on our network / admin server
- We comply with the WEEE directive on equipment disposal, supported by our School's technician, by using an approved or recommended disposal company for disposal of equipment where any protected data has been held and get a certificate of secure deletion for any server that once contained personal data
- Paper based sensitive information is collected by secure data disposal service

Personal Mobile Phones and Mobile Devices

See the guidance and requirements in the Mobile Phone Policy

Digital Images and Video

In this school

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their 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
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use

- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their IT 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

Asset Disposal

Details of all school-owned hardware will be recorded in a hardware inventory. Details of all school-owned software will be recorded in a software inventory. All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.