Haddenham Community Infant School

E Safety Policy 2021

Date Written	**March 2021**
Date adopted by Governing Body	**March 2021**
Date for next review by Curriculum	**March 2024**
Related policies	**Child Protection, Data Protection, Remote Education**

Contents

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 Haddenham Community Infant School with respect to the use of COMPUTING-based technologies.
- Safeguard and protect the children and staff of Haddenham Community Infant School and comply with GDPR (General Data Protection Regulation).
- 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

- ignoring age ratings while playing online games (exposure to violence associated with often racist/foul language, addiction, in-app purchases)
- exposure to inappropriate content, including online pornography,
- Ignoring age restrictions on social networking websites such as Instagram, Facebook, YouTube, Snapchat, WhatsApp and other apps.
- Data breach
- hate sites, sites inciting radicalisation and/or extremism
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft 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)

- Copyright (little care or consideration for intellectual property and ownership – such as music and film)
- Inappropriate Messaging

This policy applies to all members of Haddenham Community Infant School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of Haddenham Community Infant School COMPUTING systems, both in and out of Haddenham Community Infant School.

Haddenham Community Infant 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 e-safety behaviour that take place out of school.

Role	Key Responsibilities
Head	● To take overall responsibility for e-Safety provision ● To take overall responsibility for data and data security GDPR compliant ● To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements eg Bucks ● 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 eSafety incident. ● To receive regular monitoring reports about E-Safety from Computing Coordinator ● To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures
e-Safety – Computing Co-ordinator / Designated Child Protection Leader	● 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 ensures that e-safety education is embedded across the curriculum ● liaises with school COMPUTING technical staff ● To communicate regularly with SLT and the designated e-Safety Governor /

	committee to discuss current issues, review incident logs and filtering / change control logs ● To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident ● To ensure that an e-Safety incident log is kept up to date ● facilitates training and advice for all staff ● 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
Governors	● To ensure that the school follows all current e-Safety advice to keep the children and staff safe ● To approve the E-Safety Policy and review the effectiveness of the policy. 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 ● To support the school in encouraging parents and the wider community to become engaged in e-safety activities
Computing Curriculum Coordinator	● To oversee the delivery of the e-safety element of the Computing curriculum ● To address e-safety issues as they arise promptly
Network Manager/technician The school uses third party company – Turn It On	● To report any e-Safety related issues that arises, to the Computing Coordinator. ● To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy ● To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) ● To ensure the security of the school Computing 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 ● that he / she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant ● that the use of the network / remote access / email/School Twitter account is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator/Data Protection Lead /Head of School 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 e-security and technical procedures
Data Protection Lead/ Data Protection Officer	● To take overall responsibility for data and data security ● To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	● To embed e-safety issues in all aspects of the curriculum and other school activities ● To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) ● To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	● To read, understand and help promote the school's e-Safety policies and guidance ● To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy ● 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
Pupils	● Read, understand, sign and 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 e-safety practice when using digital technologies out of school and realise that the school's ESafety 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 read, understand and promote the school Pupil Acceptable Use Agreement with their children ● To access the school website /Facebook page account accordance with the relevant school Acceptable Use Agreement. ● To consult with the school if they have any concerns about their children's use of technology
External groups	● Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school ● To seek parental consent if the external party intends to use pupil photograph

Communication:

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

- Policy to be posted on the school website/ staffroom/Computing area.
- 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 whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

Handling complaints:

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. 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: o interview/counselling by teacher / Phase Leader / e-Safety Coordinator / Headteacher;

- 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]; o referral to LA / Police.

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

Complaints of cyberbullying are dealt with in accordance with our AntiBullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring

The e-safety policy is referenced from within other school policies: Computing policy, Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education policies.

The school has an e-safety coordinator who 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 school e-safety Coordinator and is current and appropriate for its intended audience and purpose.

There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders such as the PTA. All amendments to the school e- Safeguarding policy will be discussed in detail with all members of teaching staff.

Education and Curriculum

Pupil e-Safety curriculum

This school

Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHCE curriculum. It is built on Purple Mash and e-Safeguarding and e-literacy framework for EYFS to Y2.

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 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 photos 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 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.
- 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;

Staff and governor training

This school

Ensures staff and governors have had GDPR training and 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, GDPR and the school's esafety education program; Termly updates in 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 e-Safeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

This school

Runs a rolling programme of advice, guidance and training for parents to ensure that principles of e-safety behaviour are made clear, including:

- Information leaflets; in school newsletters; on the school web site;
- demonstrations, workshops, practical sessions held at school;
- 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 school, all users:

- are responsible for using the school Computing systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (at EYFS 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 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 the school's e-safety policy and using the school COMPUTING systems accordingly, including the use of mobile phones, and hand held devices.
- Are responsible for pupil data safe so that it is GDPR compliant

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 school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse
- the school does not permit parents/carers to take photographs and videos of their child/children at school events however at the end of assembly parents/carers are permitted to take photos of their own child/children only and that the school requests that photos/videos are not shared on any social networking site such as Facebook, WhatsApp, snapchat, twitter etc.

Incident Management

In this school:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and 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 the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA
- 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.
- Data breaches are reported to our Data Protection Lead (DPL) is Emma Lister/Lucy McNeil. Our Data Protection Officer (DPO) is Turn It On and if need it be then to Information Commissioners Office (ICO)
- Any safeguarding incidents are reported Designated Safeguarding Lead (DSL) Lucy McNeil or to Beckie Lewis (Deputy Safeguarding Lead)
- all the e-safety incidents are reported to the Head/Computing coordinator.
- the Head/ Computing Coordinator/Class Teacher keeps the records of the e-safety incidents.

Managing the Computing infrastructure

Internet access, security (virus protection) and filtering

The school has a managed ICT service provided by an outside contractor, Turn It On, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school Online Safety Policy / Acceptable Use Agreements. The school should also check their Local Authority/other relevant body policies on these technical issues.

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements (as outlined in Local Authority policy and guidance)
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
  Nb. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
  The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / children etc)
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place (logging with the Headteacher or the technical staff in writing) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software

- 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
- 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;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;

- 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; 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; o Informs all users that Internet use is monitored;
- Makes clear all users know and understand what the 'rules of appropriate use' are, GDPR compliance 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.
- Computing devices provided by school to members of staff are regularly checked by the IT technicians.

Network management (user access, backup)

This school

- Uses Technicians employed by Turn It On
- 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 school will conform to the GDPR requirements o Staff will only use encrypted USB sticks to hold any data about pupils

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's E-safety Policy, Data Protection Policy, Data Retention 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. Guest users do not have 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 a year group network log-in username and password.
- All pupils have their own unique username and password which gives them access to the Internet, the Learning Platform, 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 designated work areas for pupils and one for staff, including the Google Drive. 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
- 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 we also automatically switch off all computers at 6 o'clock to save energy;
- 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; 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: e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution / RAv3 system or Google Suite
- 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 (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 the DfE secure s2s website for all CTF files sent to other schools or encrypted platforms for file transfer eg egress, AnyComms
- 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 computer systems regularly with regard to health and safety and security.

Passwords policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find.
- 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 to enter our MIS systems

Emails

Staff:

- Staff only use @haddenhaminfant e-mail systems for professional purposes

- Access in school to external personal e mail accounts is not permitted and may be blocked
- Never use personal email to transfer staff or pupil personal data. We use secure @haddenhaminfant mail account.
- 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;
- All staff sign our 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.
- A letter sent to anyone using the school letterhead must be approved by the head teacher.
- Staff must not add pupils as friends in social networking sites.
- Staff must not use social networking sites within lesson times
- Staff should review and adjust their privacy settings to give them the appropriate level of privacy (See Staff Code of Conduct Document)

School website

- The Administrator 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 teaching and admin staff:
- 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, office@haddenhaminfant.bucks.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 geo-data in respect of stored images o We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

Video Conferencing

This school

- Only uses google meet and zoom supported services for video conferencing activity;
- Only uses school devices;

Data security: Management Information System access and Data transfer

Strategic and operational practices
At this school:

- Staff to report any incidents where data may have been breached Data Protection Lead and our Data Protection Officer
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset in the staff room and school office.

We ensure

- All staff are DBS checked and records are held in one central record 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
- 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 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 undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

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 / 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;
- Photos/videos taken on school iPads are stored on the school network.
- 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 identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

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 PRM Green Technologies website.

The school may also offer old IT equipment (that is deemed too slow and is no longer used by school such as an old laptop with less than I3 processor) to staff, once all the data and software including the firewall is erased by the IT technician.