E-Safety and Acceptable Use Policy for Mulberry UTC

Approval Body:	Mulberry UTC LGB
Approval Date:	November 2020
Implementation Date:	November 2021
Review Date:	November 2022
Policy Version:	4

Version	Reviewed	Changes since last version
1		
2	November 2019	• The policy has been updated to reflect the new Mulberry Schools Trust policy. References to MST staff have been added, e.g. in relation to the role of the Chief Operating Officer. • Appendix A, providing e-safety guidance to parents, has been added.
3	November 2020	• The policy has been changed to reflect the new pastoral structure and the UTC. • The policy has been changed to reflect the fact that digital learning is embedded into the curriculum of each specialism. • The policy has been changed to reflect that when mobile phones are confiscated from students they are given back the end of the day, opposed to the next day.
4	November 2021	• Removed reference to Chief Operating Officer and added reference to Director of Digital Learning • Minor updates in section 4 to reflect current practice. • Added reference in section 4 to the use of MS Teams as a VLE.

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 Mulberry UTC with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Mulberry UTC.
- 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 the Mulberry UTC community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of the school's ICT systems, both in and out of the school

The Education and Inspections Act 2006 empowers Principals/Headteachers, to such extent as is reasonable, to regulate the behaviour of students 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 cyber-bullying, or other e-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 e-safety behaviour that take place out of school.

Roles and responsibilities

Role	Key Responsibilities
Trust Director of Performance and Standards	• Takes overall responsibility for e-safety provision within the Mulberry Schools Trust • Takes overall responsibility for data and data security
Principal	• Ensures the school uses an approved filtered internet service, which complies with current statutory requirements. • Responsible for ensuring that staff receive suitable training to carry out their e-safety roles and training other colleagues, as relevant. • Aware of procedures to be followed in the event of a serious e-safety incident. • Receives regular monitoring reports from the E-Safety Co-ordinator. • Ensures there is a system in place to monitor and support staff who carry out internal e-safety procedures.
Designated Safeguarding Lead (DSL)	• Designated E-Safety Coordinator. • Day to day responsibility for e-safety issues and has a leading role in reviewing the school e-safety policy and procedures. • Communicates regularly with SLT and governors to discuss current issues, review incident logs and filtering logs. • Ensures all data held on students on school devices have appropriate access controls in place. • Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident. • Ensures that an e-safety incident log is kept up to date. • Liaises with the Local Authority and relevant agencies in relation to e-safety. • Is regularly updated about e-safety issues and legislation, and is 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.

Director of Digital Learning	• Takes an active role in reacting to reports of cyber attacks or vulnerabilities in school networks. • Promotes an awareness and commitment to e-safety throughout the school community. • Ensures that e-safety education is embedded across the curriculum. • Liaises with the school's IT technician in relation to current issues and internet filtering. • Facilitates training and advice for all staff. • Ensures the school's policy on web filtering is applied and updated on a regular basis. • 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.
Director of Pastoral Provision and Heads of House	• Oversee the delivery of the e-safety element of the Personal Development curriculum. • Liaise with the E-Safety Coordinator regularly.
School IT technician and MST network manager	• Report any e-safety related issue that arises to the DSL and the Principal. • Ensure users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed. • Ensure provision exists for misuse detection and malicious attack (e.g. keeping virus protection up to date). • Ensure the security of the school's IT systems. • Ensure access controls/encryption exist to protect personal and sensitive information held on school-owned devices. • Regularly monitor the use of the network, remote access and email in order that any misuse / attempted misuse can be reported to the DSL for investigation • Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • Keep up-to-date documentation of the school's e-security and technical procedures.
Teaching Staff	• Embed e-safety issues in all aspects of the curriculum and other school activities. • Supervise and guide students carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities). • Ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright.
All Teaching and Support Staff	• Read, understand and help promote the school's e-safety policies and guidance. • Read, understand, sign and adhere to the school staff Acceptable Use Agreement. • Are 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. • Report any suspected misuse or problem to the E-Safety Coordinator Maintain an awareness of current e-safety issues and guidance. • Model safe, responsible and professional behaviours in their own use of technology.

	• Ensure any digital communications with students is on a professional level and only through school-based systems, never through personal mechanisms, e.g. personal email, text message etc.
Students	• Read, understand, sign and adhere to the Student Acceptable Use Policy. • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • Understand the importance of reporting abuse, misuse or access to inappropriate materials. • Know what action to take if they or someone they know feels worried or vulnerable when using online technology. • Know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • Know and understand school policy on taking / using images o students and on cyber-bullying. • Understand the importance of adopting good e-safety practice when using digital technologies in and 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. • Take responsibility for learning about the benefits and risks of using the internet and other technologies safely, in school and at home. • Provide a student's perspective to help the school in the creation/ review of e-safety policies.
Local Governing Body	• Ensure the school follows all current e-safety advice to keep the children and staff safe. • Approve the E-Safety and Acceptable Use Policy and review its effectiveness. • Receive regular information about e-safety incidents and monitoring reports. • Support the school in encouraging parents and the wider community to become engaged in e-safety activities. • The role of the Safeguarding link governor will include regular review with the DSL (including e-safety incident logs and filtering logs).
Parents/carers	• Support the school in promoting e-safety. • to read, understand and promote the school Student Acceptable Use Agreement with their children. • Access the school website/online student records in accordance with the relevant school Acceptable Use Agreement. • 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.

Communication

This policy is included in the School Handbook issued to all staff annually. Acceptable Use Agreements are communicated as in the E-Safety and Acceptable Use Policy.

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 students are given information about infringements in use and possible sanctions in line with the Behaviour Policy.

Our Designated Safeguarding Lead acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Principal. Complaints related to cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school child protection procedures. We ensure all the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.

Review and Monitoring

The E-Safety and Acceptable Use Policy is related to other school policies which are available on the school website:

- Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy

The school's Designated Safeguarding Lead is responsible for the policy's review and update. The E-Safety and Acceptable Use Policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school. All amendments to the school e-safety policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Student e-safety curriculum

This school:

- has a clear, progressive e-safety education programme as part of the PSHE programme and digital learning is addressed within the curriculum in each specialist subject area. Students learn 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 website / 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;
    - 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 have strategies for dealing with receipt of inappropriate materials;
    - To understand why and how some people will 'groom' young people for sexual, political or other 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;
- plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- reminds students about their responsibilities through an Acceptable Use Agreement which every student signs;
- ensures staff model safe and responsible behaviour in their own use of technology during lessons;
- ensures that when copying materials from the web, staff and Students 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 students understand the issues around aspects of the commercial use of the internet, such as risks in pop-ups; buying on-line; on-line gaming / gambling.

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 e-safety issues and the school's e-safety curriculum

- provides, as part of the induction process, all new staff [including those on placements and work experience] with information and guidance on the e-safety policy and the Acceptable Use Policy.

Parent awareness and training

This school:

- provides clear advice, guidance and training for parents, including:
    - introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
    - information on e-safety in school newsletters and on the school website (see Appendix A for an example)
    - suggestions for safe Internet use at home supported by practical sessions held at school
    - information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will sign before being given access to school systems.

- understand the importance of misuse or access to inappropriate materials and are aware of the consequences

- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety and Acceptable Use Policy covers their actions out of school, if related to their membership of the school

- know and understand school policies on the use of mobile phones, digital cameras and hand held devices, on taking / using images of Students and on cyber-bullying

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 of the school 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 in dealing with e-safety issues

- e-safety incidents are monitored and reported and this contributes to developments in policy and practice in e-safety within the school. Records are reported to the school's Governors

- parents/carers are specifically informed of e-safety incidents involving young people for whom they are responsible;

- we contact the police if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law.

4. Managing the ICT infrastructure

Internet access, security and filtering

This school:

- uses the Fortiguard filtering system to block sites that fall into categories such as pornography, race hatred, gaming, illegal nature etc. (Details are in Appendix B)

- uses user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;

- ensures the network is healthy through use of anti-virus software etc. and the network is set-up so that executable files can be downloaded but can only be executed by someone with admin rights;

- uses LA approved systems and secure email to send personal data over the internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;

- blocks all chat rooms and social networking sites except those that are part of an educational network or approved learning platform;

- blocks Student access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;

- is vigilant in its supervision of students' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older Students have more flexible access;

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

- ensures Students only publish within an appropriately secure environment;

- plans the curriculum context for Internet use to match Students' ability, always using Google Safe Search

- informs all users that Internet use is monitored;
- informs staff and Students that that they must report any failure of the filtering systems directly to the IT technician or the DSL;
- 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 Students, staff and parents
- immediately refers any material we suspect is illegal to the appropriate authorities e.g. the 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;
- ensures the storage of all data within the school conforms to the UK data protection requirements;
- where storage of data is online and hosted within the EU, this conforms to the EU data protection directive.

To ensure the network is used safely, this school:

- ensures staff read and sign that they have understood the school's Acceptable Use of ICT Agreement. 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 use the same username and password for access to our school's network;
- controls staff access to the schools' management information system through advising staff to have a separate password for SIMS, for data security purposes;
- provides Students with their own unique username and password which gives them access to the school's network, Internet, and their own school approved email account;
- makes clear that no one should log on as another user and makes clear that Students should never be allowed to log-on or use teacher and staff logins as these have far fewer security restrictions;
- has set-up the network with a shared work area for Students and one for staff. Staff and Students are shown how to save work and access work from these areas;
- requires all users always to log off when they have finished working or are leaving the computer unattended;
- 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;

- 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;

- 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;

- ensures that access to the school's network resources from remote locations by staff is only through school 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;

- 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;

- ensures that all student 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;

- secures its wireless network to industry standard Enterprise security level;

- installs all computer equipment professionally and ensures it meets health and safety standards;

- maintains equipment to ensure Health and Safety Regulations are followed;

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

Password policy

- This school makes it clear that staff and Students must always keep their password private, must not share it with others and must not leave it where others can find it;

- All staff and Students have their own unique username and private passwords to access school systems. Staff and Students are responsible for keeping their password private.

- We require staff to use strong passwords for access to our network and MIS system and to change them once a term. We require students to change their network passwords annually.

E-mail

This school:

- provides staff with an email account for their professional use, and makes clear personal email should be through a separate account;
- provides students with an email account for educational use; does not publish personal e-mail addresses of students or staff on the school website. We use anonymous or group e-mail addresses, for example info@trustname.org / principal@schoolname.org for communication with the wider public;
- ensures that email accounts are maintained and up to date;
- will contact the police if one of our staff or students receives an e-mail that we consider is particularly disturbing or breaks the law;
- reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the police.
- uses Sophos anti-virus software and direct email filtering to protect users and systems from spam, phishing and virus attachments;

Students:

- Students are introduced to, and use e-mail as part of the Personal Development and digital learning programmes of study.
- Students are taught about the safety and 'netiquette' of using e-mail both in school and at home including:
    - 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 parent/carer or teacher;
    - that they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
    - 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, nor to delete them, 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;
    - to 'Stop and Think Before They Click' before sending or opening attachments;
    - 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;
    - not to embed adverts or forward 'chain' e-mail letters.
- Students sign the school's Acceptable 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.

Staff:

- Staff only use Trust e-mail systems for professional purposes
- Staff never use email to transfer staff or Student personal data. We use secure, LA approved systems.
- 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 and that it should follow the school 'house-style'
- The sending of multiple or large attachments should be limited; sending chain letters is not permitted; embedding adverts is not allowed;
- All staff sign the school's 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 Principal takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- Uploading information is restricted to appropriate members of the team.
- 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. Home information or individual e-mail identities will not be published.
- Photographs published on the web do not have full names attached; nor are full names used in the file names or tags when saving images.
- We expect teachers using school approved blogs or wikis to password protect them and run them 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 is made in social media to Students / Students, parents / carers or school staff;
    - they do not engage in online discussion on personal matters relating to members of the school community;
    - personal opinions are not 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.

Video

- The school only uses approved webcam sites for video conferencing activity.

- The school has CCTV in the school as part of site surveillance for staff and Student safety. We will not reveal any recordings without permission, except where disclosed to the Police as part of a criminal investigation.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

VLE - Microsoft Teams

This school:

- uses enterprise grade cloud software to provide students with a virtual learning environment;
- uses single sign on technology to ensure safe and secure access to student data. Passwords can be reset remotely in the case that a password is compromised;
- uses a VLE which encrypts data in transit and at rest;
- encourages staff and students to send data via link rather than as attachments, ensuring that only those who are authorised to have access can view files;
- syncs data from the central MIS to the VLE to ensure it is simple to keep information up to date in accordance with data protection and retention policies;
- allows staff to monitor the use of the VLE in their classes and report any concerns to the safeguarding lead;
- uses security policies to govern access to features such as chat and video calls within the VLE in line with the Trust's safeguarding policy.

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

Strategic and operational practices

At this school:

- the Mulberry Schools Trust Chief Operating Officer is the Senior Information Risk Officer, reporting to the CEO;
- we ensure staff know who to report any incidents where data protection may have been compromised;
- all staff are DBS checked and records are held in one central record;
- we ensure all the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
    - staff
    - governors
    - students
    - parents

This makes clear staff responsibilities with regard to data security, passwords and access.

- we follow LA guidelines for the transfer of any data;

- we provide secure remote access to our ICT network so that it is very rarely necessary to remove data from the school site. We require that any Protect and Restricted material be encrypted if it is to be removed from the school.
- school staff with access to setting-up usernames and passwords 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

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log out of systems or lock their screens when leaving their computer.
- We use Switch Egress to securely transfer CTF Student data files to other schools.
- All servers are in lockable locations and managed by DBS-checked staff.
- We lock any back-up tapes in a secure, fire-proof cabinet. No back-up tapes leave the site on mobile devices.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the owner's 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 off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day. Staff members may only use their phones during school break times unless they are being used for work purposes to communicate with other staff off site.
- All visitors are requested to keep their phones on silent.
- 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.
- The recording, taking and sharing of images, video and audio on any mobile phone is not permitted; except where it has been explicitly agreed otherwise by the Principal.
- 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.

Students' use of personal devices

- The school strongly advises that students should not bring mobile phones or other devices into school. However, 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.

- Students may not use mobile phones or other devices on the school site.

- If a Student breaches the school policy, the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones will be released to KS4 students at the end of the day and to Sixth Form students at the end of the same day.

- 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 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.

Staff use of personal devices

- 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.

- 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 school in a professional capacity (unless in an emergency (imminent danger) or exceptionally as agreed by the Principal).

- Staff will be issued with a school phone where contact with students, parents or carers is required. 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.

- Mobile phones and personally-owned devices must be switched off or on 'silent' mode when staff are teaching or in meetings.

- If members of staff wish to request to allow students to use their own mobile phones or a personally-owned device as part of an educational activity, this will first need to be approved by the senior leadership team.

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 joins the school;

- we do not identify students in online photographic materials or include the full names of students in the credits of any published school produced video materials / DVDs;
- if individual Student photos are used on the school web site, in the prospectus or in other high profile publications, the school obtains individual parental or Student permission;
- the school blocks/filters access to social networking sites or newsgroups, unless there is a specific approved educational purpose;
- students are taught about how images can be manipulated in their e-safety programme;
- students 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;
- students 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 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 Environment Agency website.

Appendix A: E-safety guidance for parents

Keep your children safe online

Teach your children the five key childnet SMART rules, which remind young people to be SMART online. You should go through these tips with your children.

S - SAFE
Keep safe by being careful not to give out personal information – such as your name, email, phone number, home address, or school name – to people who you don't trust online.

M - MEETING
Meeting someone you have only been in touch with online can be very dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

A - ACCEPTING
Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R - RELIABLE
Someone online may be lying about who they are, and information you find on the internet may not be reliable.

T - TELL
Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried.

Appendix B: Internet filtering procedures

Mulberry UTC's internet filtering systems are designed to ensure that our students are able to use the internet safely and that neither they, nor the reputation of the school, will be exposed to any risk deliberately or inadvertently by staff use of the internet.

These systems lie within a wider context, including our acceptable use and e-safety policies, our e-safety curriculum and appropriate supervision.

1. We use Impero internet filtering software.

2. All wired and wireless pcs and laptops access the internet via the Impero UTM (with two exceptions, see pt 10 below). No other route is available.

3. Student and staff own devices are also routed through the Impero UTM.

4. Impero categorises websites into pre-set categories; some websites remain uncategorised. Many uncategorised websites pose no risk to school users. However, all uncategorised websites are blocked to students. Staff have access to uncategorised websites but they are given a warning and must actively choose proceed to continue. The DHT responsible for ICT systems reviews each week a report of all uncategorised websites accessed with a view to:

- categorising those that are acceptable for staff use in order to reduce the number of warnings received;

- following up anything of concern through the usual routes and possibly making a decision to block a site for staff.

5. The school can choose to block particular Impero categories. We have blocked the health category for example so that we can have more control over specific websites within that category.

6. Staff wishing to use a blocked website, or a website within a blocked category, request its unblocking via the ICT helpdesk . They state whether they are requesting it for staff or Student access and what they will use it for. The vast majority of requests are for staff access only.

7. The request is passed on to the Senior Vice Principal who is the Designated Safeguarding Lead. She views the website and makes a judgement about risk. She considers:

- the provider of the website
- the scope of its content (although she does not attempt to look through the whole site)
- any chat room/blogging/commenting/forum facility
-

8. The request and the decision to unblock (or not) a site for staff, students or a sub-set of students is recorded by the ICT support team and acted upon. The unblocked website is either given an acceptable Impero category or tagged within Impero for staff use only. A list of the requests, reasons and approvals is available for scrutiny at any time. In some cases, a site may be unblocked for a limited time only.

9. The ICT support team, and no other staff, can bypass the Impero UTM for one-off arrangements, for example a particular video conferencing facility that could not be accessed through Impero.

11. In addition, a known group of individual senior staff have been given the facility to access blocked websites by entering their personal ID. The website they are accessing and their reason for doing so is logged against their ID. These records are viewed by the Senior Vice Principal responsible weekly.

12. The Senior Vice Principal, who is also the Designated Safeguarding Lead, also uses Impero reports regularly to monitor student attempts to access blocked or uncategorised websites and staff attempts to access blocked websites and to check for inappropriate or concerning searches. The reports identify the user name for each attempt/search. Subsequent action on any concern about an individual Student or group of students follows our child protection procedures.

13. We cannot currently monitor changes in internet usage pattern for individual students or staff.