



Online Safety Policy

Contents

1. Introduction and Overview

- Rationale and Scope
- Roles and responsibilities
- How the policy is communicated to staff/students/community
- Handling complaints
- Reviewing and Monitoring

2. Education and Curriculum

- Student online safety curriculum
- Staff and governor training
- Parent awareness and training

3. Expected Conduct and Incident Management

4. Managing the IT Infrastructure

- Internet access, security (virus protection) and filtering
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Learning platform
- Social networking
- Video Conferencing

5. Data Security

- Management Information System access
- Data transfer
- Asset Disposal

6. Equipment and Digital Content



- Personal mobile phones and devices
- Digital images and video

Appendices

- A1: Acceptable Use Agreement (Staff and MC members)
- A2: Acceptable Use Agreements (Students)
- A3: Image consent form (Parents)
- A4: <http://www.digitallyconfident.org/images/resources/first-line-information-support-HQ.pdf> - page 23 onwards
- A5: Search and Confiscation guidance from DfE
<https://www.gov.uk/government/publications/searching-screening-and-confiscation>



1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of Malden Oaks with respect to the use of IT-based technologies.
- Safeguard and protect the students and staff.
- Assist school staff working with students to work safely and responsibly with the Internet and other IT and 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 for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be 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
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords



Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of Malden Oaks community (including staff, students, parents/carers, visitors, community users) who have access to and are users of school IT systems, both in and out of Malden Oaks.

Roles and responsibilities

Role	Key Responsibilities
Headteacher	<ul style="list-style-type: none"> • Is adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • To lead a ‘safeguarding’ culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security (SIRO) ensuring school’s provision follows best practice in information handling • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident • Ensure suitable ‘risk assessments’ undertaken so the curriculum meets needs of students, including risk of students being



Role	Key Responsibilities
	radicalised <ul style="list-style-type: none"> • To receive regular monitoring reports from the Online Safety Co-ordinator • 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 • To ensure Management Committee members are regularly updated on the nature and effectiveness of the school’s arrangements for online safety • To ensure school website includes relevant information.
Online Safety Co-ordinator/Designated Child Protection Lead (This may be the same person)	<ul style="list-style-type: none"> • Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school’s online safety policy/documents • Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the curriculum • Liaise with school technical staff where appropriate • To communicate regularly with SLT and the designated online 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 online safety incident • To ensure that online safety incidents are logged as a safeguarding incident • Facilitate training and advice for all staff • Oversee any student surveys / student feedback on online safety issues • Liaise with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
MC members/Safeguarding	<ul style="list-style-type: none"> • To ensure that the school has in place policies and practices to keep the students and staff safe online



Role	Key Responsibilities
governor (including online safety)	<ul style="list-style-type: none"> • To approve the Online Safety Policy and review the effectiveness of the policy • To support the school in encouraging parents and the wider community to become engaged in online safety activities • The role of the online safety Governor will include: regular review with the online safety Co-ordinator.
Computing Curriculum Leader	<ul style="list-style-type: none"> • To oversee the delivery of the online safety element of the Computing curriculum
Network technician / School Business Manager	<ul style="list-style-type: none"> • To report online safety related issues that come to their attention, to the Online Safety Coordinator • To manage the school’s computer systems, ensuring <ul style="list-style-type: none"> - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - 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 they keep 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 school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school’s online security and technical procedures
Data and Information (Asset Owners) Managers (IAOs)	<ul style="list-style-type: none"> • To ensure that the data they manage is accurate and up-to-date • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • The school is registered with Information Commissioner
LGfL Nominated	<ul style="list-style-type: none"> • To ensure all LGfL services are managed on behalf of the school



Role	Key Responsibilities
contact(s)	following data handling procedures as relevant
Teachers	<ul style="list-style-type: none"> • To embed online safety in the curriculum • To supervise and guide students carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff, MC members and contractors.	<ul style="list-style-type: none"> • To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction. • 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 <p>Exit strategy</p> <ul style="list-style-type: none"> • At the end of the period of employment to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Students	<ul style="list-style-type: none"> • Read, understand, sign and adhere to the Student Acceptable Use Policy annually • 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 understand the importance of adopting safe behaviours and 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 • To contribute to any 'student voice' / surveys that gathers



Role	Key Responsibilities
	information of their online experiences
Parents/carers	<ul style="list-style-type: none"> • To read, understand and promote the school’s Student Acceptable Use Agreement • to consult with the school if they have any concerns about the use of technology • to support the school in promoting online safety and endorse the Acceptable Use Agreement which includes the students use of the Internet and the school’s use of photographic and video images
External groups	<ul style="list-style-type: none"> • Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school • to support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology.

Communication:

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

- Policy to be posted on the school website
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and students at the start of each year and to be issued to whole school community, on entry to the school.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Staff and students are given information about infringements in use and possible sanctions.
- Online Safety Coordinator acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Coordinator that day



- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Management Committee members and the LADO (Local Authority's Designated Officer).

Handling a sexting / nude selfie incident:

[UKCCIS "Sexting in schools and colleges"](#) should be used. This extract gives the initial actions that should be taken:

There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people
When assessing the risks the following should be considered:
 - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
 - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
 - Are there any adults involved in the sharing of imagery?
 - What is the impact on the pupils involved?
 - Do the pupils involved have additional vulnerabilities?
 - Does the young person understand consent?
 - Has the young person taken part in this kind of activity before?
- If a referral should be made to the police and/or children's social care
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult



2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The imagery involves sexual acts
5. You have reason to believe a student is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply, then a school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support.

Review and Monitoring

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Management Committee members. All amendments to the school online safety policy will be disseminated to all members of staff and students.

2. Education and Curriculum

Student on line safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind students about their responsibilities through the student Acceptable Use Agreement



- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure students only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program;
- provides, as part of the induction process, all new staff with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras;

Staff and contractors



- know to be vigilant in the supervision of students at all times, as far as is reasonable.
- know to take professional, reasonable precautions when working with students, previewing websites before use; using age-appropriate (student friendly) search engines where more open Internet searching is required;

Parents/Carers

- should provide consent for students to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- should know and understand what the school's 'rules of appropriate use for the whole school community' 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;
- all members of the school 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 (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use is monitored;
- has the educational filtered secure broadband connectivity through the LGfL;



- uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- ensures network health through use of Sophos anti-virus software
- Uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users - the LGfL USO system;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- 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;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to [DfE guidance](#);
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data 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. The same credentials are used to access the school's network.
- All students have their own unique username and password which gives them access to the Internet and other services;
- 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;



- 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 to log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and 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 audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- 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 or through USO secure file exchange (USO FX);
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy

- This school makes it clear that staff and students must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to change their passwords into the MIS, LGfL USO admin site on a regular basis.

E-mail



This school

- Provides staff with an email account for their professional use, London Staffmail and makes clear personal email should be through a separate account;
- 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.
- Will ensure that email accounts are maintained and up to date
- We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Students:

- We use LGfL studentemail system which are intentionally 'anonymised' for student protection.
- Students are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff can only use the LA or LGfL e mail systems on the school system
- Staff will use LA or LGfL e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Never use email to transfer staff or student personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

- The Head teacher, supported by the Management Committee, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with statutory DFE requirements;
- 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;
- Photographs published on the web do not have full names attached. We do not use students' names when saving images in the file names or in the tags when publishing to the school website;

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.



- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students, parents/carers or school staff;
- School staff should not be online friends with any student. Any exceptions must be approved by the Headteacher.
- 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 and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Students:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our student Acceptable Use Agreement.

Parents:

- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.

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

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- 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 owners.



- 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 a single central record

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content.
- All servers are in lockable locations and managed by DBS-checked staff.
- 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.
- 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.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into school are entirely at the staff member, students & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from Headteacher / SLT.
- Student personal mobile devices, 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 during lessons.
- The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices.
- Personal mobile devices will only be used during lessons with permission from the teacher.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- All visitors are requested to keep their phones on silent.



- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobiles devices may be searched at any time as part of routine monitoring.
- 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.

Storage, Synching and Access

The device is accessed with a school owned account

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the network manager.

The device is accessed with a personal account

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the network manager.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Students' use of personal devices

- The School advises that if student mobile phones and devices are brought into school this is entirely at their own risk/responsibility.
- If a student breaches school policy, then their mobile phone may be confiscated at the start of each day for a period of time and will be held in a secure place in the school office. Mobile devices will be released at the end of the day.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.



- 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 are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting students, young people or their families within or outside of the setting.
- Staff will be issued with a school phone where contact with students, parents or carers is required, for instance for off-site activities.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow students to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- 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 and then report the incident with the Headteacher / Designated Officer.
- If a member of staff breaches the school policy then disciplinary action may be taken.

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 students in online photographic materials or include the full names of students in the credits of any published school produced video materials/DVDs;
- 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 students;
- If specific student 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 student permission for its long term, high profile use



- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Students are taught about how images can be manipulated in their online safety education 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. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Date agreed by the Management Committee:

Agreed date for Next Review:



APPENDIX 1

Acceptable Use Agreement:

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable'.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
- I will only use the approved communication systems (email/T2P) with students or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that may be considered offensive or of an extremist nature.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the School Business Manager or Head Teacher.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- **I will not connect any device (including USB flash drive)**, to the network that does not have up-to-date anti-virus software.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of students or staff and will not store any such images or videos at home.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the appropriate system or staff-only drive within school.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.



- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any “significant personal use” as defined by HM Revenue & Customs.
- I will only access school resources remotely (such as from home) using the LGfL system and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or student information, held within the school’s information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or students, which I believe may be inappropriate or concerning in any way, to the Designated Safeguarding Lead (Alison Vigor) / or SLT.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Head / SLT on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- **Staff that have a teaching role only:** I will embed the school’s on-line safety / digital literacy / anti radicalisation curriculum into my teaching.

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a ‘safe and responsible digital technologies user’. I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school’s most recent e-safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature Date

Full Name:

APPENDIX 2

ICT STUDENT AGREEMENT

These rules will keep everyone safe and help us to be fair to others.



1. I will only use the school's computers for appropriate school activities and learning and am aware that the school can monitor my internet use.
2. I will not bring files into school that can harm the school network or be used to circumvent school security tools
3. I will only edit or delete my own files and not view, or change, other people's files or user areas without their permission.
4. I will keep my logins, IDs and passwords secret and change my password regularly.
5. I will use the Internet responsibly and will not visit web sites that are inappropriate for the school or my key stage.
6. I will only e-mail or contact people I know, or those approved as part of learning activities
7. The messages I send, or information I upload, will always be polite and sensible. All messages I send reflect on me and the school.
8. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will never open a file.
9. I will not give my personal information that could be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.
10. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me.
11. If I see anything I am unhappy with or I receive a message that makes me feel uncomfortable, I will not respond to it but I will save it and talk to a trusted adult.
12. I am aware that some websites, games and social networks have age restrictions and I should respect this.
13. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.

I have read and understand these rules and agree to them.

Signed: Date:

Appendix 3

Consent Form

Name of Child: _____

1) IMAGE CONSENT

Occasionally, we may take photographs or videos of the students at the school. We may use these images in our school's prospectus, in other printed publications that we produce, for educational use and possibly on our website.



To comply with the Data Protection Act 1988, we need your permission before we can photograph or make any recordings of your child. Please answer the questions below, then sign and date the form where shown and return the completed form to the school.

Please circle your answer

May we use your child's photograph in the school prospectus and other printed publications that we produce? **Yes / No**

May we use your child's image on our website? **Yes / No**

May we record your child's image on video? **Yes / No**

Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK law applies.

Please note that the conditions for use of these photographs are on the back of this form.

I have read and understood the conditions of use on the back of this form.

Parent's or Carer's signature: _____ Date: _____

Name (capitals): _____

APPENDIX 4

<http://www.digitallyconfident.org/images/resources/first-line-information-support-HQ.pdf>

page 23 onwards

APPENDIX 5

Search and Confiscation guidance from DfE

<https://www.gov.uk/government/publications/searching-screening-and-confiscation>