Walthamstow School For Girls

"Neglect not the gift that is in thee"

Policy Document

E-Safety Policy

Author(s):	**Dave Shackson**
Ratification Date:	**6th December, 2016**
Next Review Date:	**TBC**
Reference:	**ES_POLICY_V2.0**

CONTENTS PAGE

THE POLICY

APPENDICES

1. INTRODUCTION AND OVERVIEW

1.1 Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Walthamstow School for Girls with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Walthamstow School for Girls.
- 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:

1.2 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.

1.3 Contact

- Grooming.
- Radicalisation.
- Cyber-bullying in all forms.
- Identity theft (including false social media accounts) and sharing passwords.

1.4 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).

1.5 Scope

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

The Education and Inspections Act 2006 empowers 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 are 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.

The school will deal with such incidents within this policy and within associated Positive Behaviour for Learning and Anti-Bullying Policies pertaining to staff and students and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-safety provision. • To take overall responsibility for data and data security (SIRO). • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL. • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant. • To be aware of procedures to be followed in the event of a serious e-safety incident. • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. ICT Systems and Network Manager).
Leadership Team member with responsibility for E-Safety (E-Safety Coordinator)	• Take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents. • Promote an awareness and commitment to e-safeguarding throughout the school community. • Ensure that e-safety education is embedded across the curriculum. • Liaise with school ICT technical staff. • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident. • Facilitate training and advice for all staff. • Liaise with the Local Authority and relevant agencies. • To keep up to date with e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: o Sharing of personal data. o Access to illegal/inappropriate materials. o Inappropriate on-line contact with adults/strangers. o Potential or actual incidents of grooming. o Cyber-bullying and use of social media. • Report e-safety incidents that involve issues of Child Protection to the designated named Child Protection Officer. • Review and decide on requests to unblock filtered online content.
Governors	• To ensure that the school follows all current e-safety advice to keep students and staff safe. • To approve the E-Safety Policy and review the effectiveness of the policy. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities.
Director of ICT	• To oversee the delivery of the e-safety element of the Computing curriculum and ensure that it meets the needs of WSFG students. • To liaise with the e-safety coordinator regularly. • To ensure that all data held on pupils on the Learning Platform is adequately protected. • To support other teachers, when required, to embed e-safety in their curriculum.

Role	Key Responsibilities
ICT Systems and Network Manager and ICT Support Officers	• To report any e-safety related issues that arise, to the Leadership Team. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed. • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date. • To ensure the security of the school ICT system. • To ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices. • To ensure that the school's policy on web filtering is applied and updated on a regular basis. • To inform LGfL of issues relating to the filtering applied by the Grid. • To keep 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. • To regularly monitor the use of the network, Learning Platform, remote access and email in order that any misuse/attempted misuse can be reported to the Leadership Team. • 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. • To refer requests to unblock filtered online content to the Leadership Team member with responsibility for e-safety. • To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts. • To ensure the integrity and security of the school website. • To refer requests to unblock filtered online content to the Leadership Team member with responsibility for e-safety.
Data Manager	• To ensure that all systems holding data on pupils 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, monitor their use and implement current school policies with regard to these devices. • To report any suspected misuse or problem pertaining to student behaviour to the relevant HoF or SPL. • To report any other suspected misuse or problem.

Role	Key Responsibilities
	- 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.
HoFs & SPLs	- To report any suspected misuse or problem to the member of the Leadership Team with responsibility for e-safety.
Pupils	- Read, understand, sign and adhere to the Student Acceptable Use Agreement. - 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 e-safety policy covers their actions out of school, if related to their membership of the school. - To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home. - To help the school in the creation/review of e-safety policies.
Parents/Carers	- To support the school in promoting e-safety and endorse the Parent Acceptable Use Agreement, which covers students' use of the Internet and the school's use of photographic and video images - To read, understand and promote the school Student Acceptable Use Agreement with their children. - To access any school systems with parental access (e.g. SIMS Learning Gateway) in accordance with the Parent Acceptable Use Agreement. - To consult with the school if they have any concerns about their child's use of technology.
External groups	- Any external individual/organisation will sign an Acceptable Use Agreement prior to using any equipment or the Internet within school.

1.6 Communication

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

- Policy to be posted on the school website and Fronter Learning Platform.
- 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.

1.7 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:
    - Interview/counselling by tutor/SPL/Leadership Team Member/Headteacher.
    - Informing parents/carers
    - Removal of Internet or computer access for a period (which could ultimately prevent access to files held on the system, including examination coursework).
    - Referral to LA/Police.
    - Other sanctions in line with those contained in the Positive Behaviour for Learning Policy.
- The member of the Leadership Team with responsibility for e-safety acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to Child Protection are dealt with in accordance with school and LA Child Protection procedures.

1.8 Review and Monitoring

The E-Safety Policy is referenced from within other school 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.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school E-Safety Policy will be discussed in detail with all members of teaching staff.

2. EDUCATION AND CURRICULUM

2.1 Pupil E-Safety Curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Computing/PSHE curriculum. This covers a range of skills and behaviours appropriate to students' 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.
    - (for older pupils) To understand how search engines work and to understand that this affects the results they see at the top of the listings.
    - To understand acceptable behaviour when using an online environment/e-mail, i.e. be polite, no bad or abusive language or other inappropriate behaviour. Keeping personal information private.
    - To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
    - To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments.
    - To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.

    - To understand why they must not post pictures or videos of others without their permission.
    - To know not to download any files – such as music files - without permission.
    - To have strategies for dealing with receipt of inappropriate materials.
    - (for older pupils) To understand why and how some people will 'groom' young people for sexual reasons.
    - To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
    - To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies i.e. parent/carer, teacher or trusted staff member, or an organisation such as Childline or the by clicking the CEOP Report button.
- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through a Student Acceptable Use Agreement which every student will sign/will be displayed throughout the school and will be displayed when a student logs on to the school network.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the Internet, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights.
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming/gambling.

2.2 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 sensitivity requires data protection.
- Makes regular information available to staff on e-safety issues.
- 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-Safety Policy and the school's Acceptable Use Agreements.

2.3 Parent Awareness and Training

This school

- Provides advice and guidance for parents, including
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear.
    - Information leaflets, The Greensheet, on the school web site.
    - Suggestions for safe Internet use at home.
    - Provision of information about national support sites for parents.

3. EXPECTED CONDUCT AND INCIDENT MANAGEMENT

3.1 Expected conduct

In this school, all users

- Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Agreement, which they will be expected to sign before being given access to school systems.
- 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 other handheld 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 ICT systems accordingly, including the use of mobile phones, and hand held devices.
- Students 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 by signing the Parent Acceptable Use Agreement at the 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.

3.2 Social Networking and Private Email

- Staff 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 should never give current students their personal email and should not communicate with students except through the school-provided systems.
- On invitational social media (e.g. to "friend" on Facebook) school staff must not invite students to be part of their social media network or accept an invitation from a current student.
- On open social media networks (e.g. twitter) staff are not required to actively block current students but should never send or respond to a direct message from a current student or a person they suspect is a current student. If a school staff member persistently receives direct messages from a current student or is concerned about public comments being made by a current student that are linked to their social media space they should report it to the Leadership Team member responsible for e-safety or, in the case of a highly sensitive matter, the Headteacher.
- Staff should not participate in online gaming with students and should not share their online nicknames with students. Where staff become aware that they are part of the same game community as a student, they should not participate in games with that student (e.g. playing co-op or Player v Player).
- School staff will ensure that in private use:
    - No reference should be made in social media to 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 should not be attributed to the school or local authority.
    - Their online presence is in accordance with the Staff Code of Conduct.
    - Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

3.3 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 a 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 (e.g. the local authority and LGFL) in dealing with e-safety issues.
- Monitoring and reporting of e-safety incidents takes place and contributes to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's Leadership Team and Governors.

- Parents/carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

4. MANAGING THE ICT INFRASTRUCTURE

4.1 Internet Access, Security (Virus Protection) and Filtering

This school

- Has educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network.
- Uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status.
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age/stage of the students.
- Ensures network health through use of Sophos anti-virus software (from LGfL) etc. and network set-up, so staff and pupils cannot download executable files.
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX and secured email to send personal data over the Internet and uses encrypted devices or secure remote access where 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.
- Only unblocks other external social networking sites for specific purposes/Internet Literacy lessons.
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network.
- Uses security time-outs on Internet access where practicable/useful,
- Works in partnership with LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.
- 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 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.
- Ensures pupils only publish within an appropriately secure environment.
- Requires staff to preview websites before use.
- Is vigilant when conducting 'raw' image searches with students e.g. Google image search.
- Informs all users that Internet use is monitored.
- Informs staff and students that that they must report any failure of the filtering systems.
- Ensures all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programmes.
- Provides advice and information on ways of reporting offensive materials, abuse bullying etc. that are available for pupils, staff and parents.
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police and the LA.

4.2 Network Management (User Access, Backup)

This school

- Uses individual, audited log-ins for all users - the London USO system.
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services.
- Uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful.
- Has additional local network auditing software installed.

- Ensures the ICT Systems and Network Manager is up-to-date with LGfL services and policies to be up-to-date with LGfL services and policies.
- Storage of all data within the school will conform to the UK Data Protection requirements.
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU Data Protection Directive, where storage is hosted within the EU.

To ensure the network is used safely, this school

- Ensures staff read and sign that they have understood the school's E-Safety Policy. Following this, they are set-up with Internet, e-mail and network access. Online access is through a unique, audited username and password.
- Controls staff access to the schools' management information system through a separate password for data security purposes.
- Provides pupils with an individual network log-in username and password.
- Provides all pupils with their own unique username and password which gives them access to the Internet, the Learning Platform and their own school approved email account.
- Uses the London Grid for Learning's Unified Sign-On (USO) system for username and passwords.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on as or use teacher/staff logins, as these have far less security restrictions and inappropriate use could damage files or the network.
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save and access work from these areas.
- Requires all users to always log off when they have finished working or are leaving the computer unattended.
- Require users to always log-off and then log-on again as themselves should they find a logged-on machine.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day.
- Has set-up the network so that users cannot download executable files/programmes.
- Has blocked student access to music/media download or shopping sites – except those approved for educational purposes.
- Scans all mobile equipment with anti-virus/spyware before it is connected to the network.
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Makes clear that staff accessing LA systems do so in accordance with any corporate policies.
- Maintains equipment to ensure Health and Safety is followed e.g. projector filters cleaned by Site Services Officers or Technicians, 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 can access SEN data.
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school/LA approved systems.
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child.
- 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 Critical Incident Plan in place covering critical data that includes a secure, remote back up of critical data which complies with external audit requirements.
- Uses our broadband network for our CCTV system and have had this set-up by approved partners.
- Uses the DfE secure s2s website for all CTF files sent to other schools.
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX).
- Follows ISP advice on Local Area and Wide Area security matters and that firewalls and routers have been configured to prevent unauthorised use of our network.
- Has secured our wireless network to industry standard Enterprise security level/appropriate standards suitable for educational use.
- Installs all computer equipment professionally and meets Health & Safety standards.
- Maintains projectors so that the quality of presentation remains high.
- Reviews the school ICT systems regularly with regard to Health & Safety and security.

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

4.4 E-Mail

This school:

- Provides staff with an email account for their professional use.
- Provides students with an email for educational use.
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk, head@schoolname.la.sch.uk or class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date.
- Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e-mails dangerous. 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, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our Internet access.

Students:

- We use LGfL LondonMail with pupils and lock this down where appropriate using LGfL SafeMail rules.
- Students' LGfL LondonMail e-mail accounts are intentionally 'anonymised' for their protection.
- Students are introduced to, and use e-mail as part of the ICT/Computing scheme of work.
- Students can only receive and send external mail if the SafeMail rules have been set to allow this.
- Students are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
    - Not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and who is approved by their teacher or parent/carer.
    - That an e-mail is a form of publishing where the message should be clear, short and concise.
    - That any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
    - That they must not reveal private details of themselves or others in e-mail, such as address, telephone number etc.

    - To ‘stop and think before you click’ and not to open attachments unless they are sure that the source is safe.
    - That they should think carefully before sending any attachments.
    - That embedding adverts is not allowed.
    - That they must immediately tell a teacher/responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature.
    - Not to respond to malicious or threatening messages.
    - Not to delete malicious of threatening e-mails, but to keep them as evidence of bullying.
    - Not to arrange to meet anyone they meet through e-mail without having discussed this with an adult and taking a responsible adult with them.
    - That forwarding ‘chain’ e-mail letters is not permitted.

Staff:

- Staff can only use the LA or LGfL e mail systems on the school system.
- Staff only use LA or LGfL e-mail systems for professional purposes.
- Access in school to external personal e-mail accounts may be blocked.
- Staff use a ‘closed’ LA email system which is used for LA communications and some ‘LA approved’ transfers of information.
- Never use email to transfer staff or pupil personal data. We use secure, LA/DfE approved systems. These include: S2S (for school to school transfer), Collect, USO-FX etc.
- 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 LA /Staff Acceptable Use Agreement to say they have read and understood the e-safety rules, including e-mail usage and we explain how any inappropriate use will be dealt with.

4.5 School website

- The Headteacher takes overall responsibility for ensuring that the website content is accurate and the quality of presentation is maintained.
- Uploading of information is restricted to our staff website administrators, who have been approved by the Senior Leadership 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 a general e-mail contact address.
- Home information or individual e-mail identities will not be published.
- Photographs published on the web do not have full names attached.
- We do not use pupils’ names when saving images in the file names or in the tags when publishing to the school website.
- We do not use embedded geodata in respect of stored images.
- We expect teachers using school approved blogs, social media platforms or wikis to password protect them and run them from a link on the school website/MLE.

4.6 Learning Platform (MLE)

- Uploading of information on the schools’ Learning Platform/MLE is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas.
- Photographs and videos uploaded to the schools’ Learning Platform/MLE will only be accessible to members of the school community through their secure MLE log-in.

- In school, pupils are only able to upload and publish to school approved and closed systems, such as the Learning Platform/MLE.

4.7 Social networking

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

- School staff will ensure that in private use:
    - No reference should be made in social media to students, parents/carers or school staff.
    - They do not engage in online discussion on personal matters relating to members of the school community.
    - Personal opinions should not be attributed to the school or Local Authority.
    - Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

4.8 Video Conferencing

This school

- Only uses the LGfL supported services for video conferencing activity.
- Only uses approved or checked webcam sites.

4.9 CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation.

5. EQUIPMENT AND DIGITAL CONTENT

5.1 Personal Mobile Phones and Mobile Devices

- Student mobile phones which are brought into school must be turned off and handed in to the front office before school and collected at the end of the school day.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any private mobile phone is not allowed; except where it has been explicitly agreed otherwise by the Headteacher or is part of a lesson or educational activity using a school-registered device. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone.
- Staff mobile phones and personally-owned devices will not be used in any way during lessons. They should be switched off or on silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- On school premises no images or videos should be taken on mobile phones or personally-owned mobile devices. In approved exceptional circumstances such as school trips or other special events no images or videos should be taken on mobile phones without the prior consent of the person or people concerned.

5.2 Students' Use of Personal Devices

- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his or her parent/carer, 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 the safe and appropriate use of mobile phones and personally-owned devices and will be made aware of rules and sanctions.

5.3 Staff Use of Personal Devices

- Staff handheld devices for use in school, including mobile phones and cameras must be noted in school – name, make & model, serial number. Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Mobile phones and other 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 children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the 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 school-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

5.4 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 home/school agreement form when their daughter 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.
- Staff sign the school's Acceptable Use Agreement and this includes a clause on the use of mobile phones/personal equipment for taking pictures of students.
- We block/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their e-safety education programme and are also taught to consider how to publish for a wide range of audiences which might include Governors, parents or younger children as part of their ICT scheme of work.
- Pupils are advised to be very careful about placing any personal photos on any social online network space. They are taught to understand the need to maintain privacy settings so as not to make their personal information public.

- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the 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.

5.5 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

<u>School Advice to Staff on Use of Social Media and Online Gaming</u>

In most cases staff can avoid problems and avoid infringing the school's E-Safety Policy by applying principles based on whether the activity they are engaged in is fully public and open, or private and by direct contact or invitation.

Using Social Media for School Purposes

Staff wanting to set up sites/areas on social media platforms for educational use should only do so with the school's approval. It is important that any such use is known by the school and can be monitored. Staff who set up unmonitored social media areas leave themselves very vulnerable and need to be aware that monitoring is as much for their protection as well as students'.

Private Use of Social Media

Staff need to be aware that, for our students and younger generations in general, social media is not just a form of communication: it is a way of socialising. The same appropriate conduct that you would apply in actual socialising needs to apply in virtual socialising. In the same way that it would be unacceptable for you to ask a student to join you and a group of your friends for a social activity, it is equally unacceptable for you to invite students into your social media activities.

In practice this means that staff should not "friend" students on sites like Facebook. It is also not advisable to "friend" unknown requests as these could be linked to students.

With regard to "open" social media, (e.g. Twitter), staff are not required to block students when they become aware of them (e.g. they "follow" you on Twitter.) This type of social media is very much like meeting in a public place. You would not be expected to ignore a student if you ran into them in public. However as it is a public place, staff need to be mindful of the comments and opinions they express on such social media. In all cases, it is unacceptable to respond to or initiate any private messaging in the same way as it is unacceptable to contact students using private email. Furthermore, staff should not actively "follow" students on social media such as Twitter.

If staff have any concerns about their potential or actual interaction with students on social media they should speak to the Leadership Team member with responsibility for e-safety.

Online Gaming

Staff should take all precautions to avoid students being able to identify them in online games (e.g. sharing nicknames, character names with students.)

If staff become aware that they are part of the same game or gaming community as a student they are not expected to quit that game or community. However, they must not engage in groups with the student (as these are by nature private and invitational) such as co-op gaming, Player v Player, guild membership or closed "instances." As a basic rule, if you are part of a closed "group" communication channel with that student instead of the fully public channel, then this is not appropriate.

Although not expected, it is advisable that when staff become aware they are in the same game or community as a student, they should consider moving their account/character to an alternate server where that is available.