Walderslade Girls' School
Online Safety Policy
(incorporating Student, Parent, Staff and Visitor Acceptalbe Use Policy)

Introduction

Aim of this policy

- Walderslade Girls' School (the School) believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles.

- The School identifies that the internet and information communication technologies are an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.

- The School has a duty to provide the school community with quality Internet access to raise education standards, promote student achievement, support professional work of staff and enhance the schools management functions. The School also identifies that with this there is a clear duty to ensure that children are protected from potential harm online.

- The purpose of this Online Safety Policy is to:

    - Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that the School is a safe and secure environment.
    - Safeguard and protect all members of the School's community online.
    - Raise awareness with all members of the School's community regarding the potential risks as well as benefits of technology.
    - To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
    - Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

- This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop or mobile phone.

- This policy must be read in conjunction with other relevant school policies including (but not limited to) Safeguarding, Anti-bullying, Behaviour, Photographic Image Use, Acceptable Use Policies, confidentiality, screening, searching and relevant curriculum policies including computing, Personal Social Health and Citizenship Education (PSHCE), and Spiritual, Moral, Social and Cultural Development (SMSC).

This Online Safety Policy has been written by the School, building on KCC advice with specialist advice and input as required.

- The policy has been approved and agreed by the SLT and Governing Body (GB).
- The School has appointed a member of the Senior Leadership Team (SLT) as the online safety lead.
- The School's Online Safety (e-Safety) Policy and its implementation will be reviewed at least annually or sooner if required.

The School's Online Safety (e-Safety) Coordinator and Designated Safeguarding Lead (DSL) is Emma Ranson, Assistant Headteacher: Guidance, Care and Inclusion.

1.2 Key responsibilities of the community

1.2.1 Key responsibilities of SLT are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
- Supporting the online safety (e-Safety) lead in the development of an online safety culture within the school.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety.
- To ensure that suitable, age-appropriate and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the school community and ensuring that the filtering and school network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all students to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- Making appropriate resources available to support the development of an online safety culture.
- Taking responsibility for online safety incidents and liaising with external agencies as appropriate.
- Receiving and regularly reviewing online safety incident logs and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.

- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To work with and support technical staff in monitoring the safety and security of schools systems and networks.
- To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.

1.2.2 Key responsibilities of the designated safeguarding/online safety lead are:

- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the school's lead for data protection and data security to ensure that practice is in line with legislation.
- Maintaining an online safety incident/action log to record incidents and actions taken as part of the schools safeguarding recording structures and mechanisms. This will be in the safeguarding and child protection folders.
- Monitor the school's online safety incidents to identify gaps/trends and update the education response to reflect need and to report to SLT, Governing Body and other agencies as appropriate.
- Liaising with the local authority and other local and national bodies as appropriate.
- Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other procedures on a regular basis (at least annually) with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.
- Meet regularly with the governor with a lead responsibility for online safety.

1.2.3 Key responsibilities of staff are:

- Contributing to the development of online safety policies.
- Reading the School's AUPs and adhering to them.
- Taking responsibility for the security of school/ systems and data.
- Having an awareness of online safety issues, and how they relate to the children in their care.
- Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives.
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern, and taking appropriate action by working with the DSL.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Taking personal responsibility for professional development in this area.

1.2.4. Additional responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with SLT.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- To ensure all staff are aware of the need to encrypt personal and sensitive information.
- Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the online safety lead and DSL.
- Ensuring that the use of the School's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the online safety lead and DSL.
- Report any breaches or concerns to the DSL and SLT and together ensure that they are recorded on the e-Safety Incident Log, and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the online safety lead and SLT, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the School's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

1.2.5 Key responsibilities of children and young people are:

- Reading the School's Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.2.6. Key responsibilities of parents and carers are:

- Reading the School's AUPs, encouraging their children to adhere to them, and adhering to them themselves where appropriate.

- Discussing online safety issues with their children, supporting the School in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of new and emerging technology.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the School, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the School's online safety policies.
- Using the School's systems, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2. Online Communication and Safer Use of Technology

2.1 Managing the Walderslade Girls' School website

- The School will ensure that information posted on the School's website meets the requirements as identified by the Department for Education.
- The contact details on the website will be the School's address, email and telephone number. Staff or students' personal information will not be published, unless consent has been given.
- The Headteacher will take overall editorial responsibility for online content published by the School and will ensure that content published is accurate and appropriate.
- The School's website will comply with the School's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- Students work will only be published with their permission or that of their parents/carers.
- The administrator account for the School website will be safeguarded with an appropriately strong password.
- The School will post information about safeguarding, including online safety on the school website.

2.2 Publishing images and videos online

- The School will ensure that all images are used in accordance with the School's Photographic Image Use Policy.
- In line with the School's Photographic Image Policy, written permission from parents or carers will always be obtained before images/videos of students are electronically published.

2.3 Managing email

- Students may only use school provided email accounts for educational purposes.
- All members of staff are provided with a specific school email address to use for any official communication.
- The use of personal email addresses by staff for any official school business is not permitted.

- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods.
- Members of the School community must immediately tell a designated member of staff if they receive offensive communication.
- Sensitive or personal information will only be shared via email in accordance with data protection legislation.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully before sending, in the same way as a letter written on school headed paper would be.
- The School will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

2.4 Official videoconferencing and webcam use

- All videoconferencing equipment in the classroom will be switched off when not in use and where appropriate, not set to auto answer.
- Equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses will not be made available to other sites.
- Videoconferencing contact information will not be put on the School's website.
- The equipment will be kept securely and if necessary locked away when not in use.
- Responsibility for the use of the videoconferencing equipment outside school time will be established with care.
- Staff will ensure that external videoconference are suitably risk assessed and that accounts and systems used to access events are appropriately safe and secure.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

Users

- Students will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately for the students' age and ability. (schools should list how this will be enforced and achieved)
- Parents and carers consent will be obtained prior to children taking part in videoconferences.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely.
- If third party materials are to be included, the School will check that recording is acceptable to avoid infringing the third party intellectual property rights.
- The School will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site the School will check that they are delivering material that is appropriate for the class.

2.5 Appropriate and safe classroom use of the internet and associated devices

- The School's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of students.
- Students will use age and ability appropriate tools to search the Internet for content.
- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.
- The School will ensure that the use of Internet-derived materials by staff and students complies with copyright law and acknowledge the source of information.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Students will be appropriately supervised when using technology, according to their ability and understanding.
- All school owned devices will be used in accordance with the School's AUP and with appropriate safety and security measure in place.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The School will use age appropriate search tools as decided by the School following an informed risk assessment to identify which tool best suits the needs of our community.
- The School will use the internet to enable students and staff to communicate and collaborate in a safe and secure environment.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school/setting requirement across the curriculum.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

2.6 Management of school portals and gateways

- SLT and staff will regularly monitor the usage of the School portal by students and staff in all areas, in particular message and communication tools and publishing facilities.

- Only members of the current student, parent/carers and staff community will have access to the portal.
- All users will be mindful of copyright issues and will only upload appropriate content onto the portal.
- When staff, students etc. leave the School their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns about content on the portal may be recorded and dealt with in the following ways:
  - The user will be asked to remove any material deemed to be inappropriate or offensive.
  - The material will be removed by the site administrator if the user does not comply.
  - Access to the portal for the user may be suspended.
  - The user will need to discuss the issues with a member of leadership before reinstatement. A student's parent/carer may be informed.
  - A visitor may be invited onto the portal by a member of the leadership. In this instance there may be an agreed focus or a limited time slot.
  - Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.

3. Social Media Policy

3.1. General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of the School community and exist in order to safeguard both the School and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of the School community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the School community.
- All members of the School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The School will control students and staff access to social media and social networking sites whilst on site and using school provided devices and systems.
- The use of social networking applications during school hours for personal use is/is not permitted.
- Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of the School community on social media sites should be reported to the SLT and will be managed in accordance with existing school policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

- Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with the relevant school policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

3.2 Official use of social media

- Official use of social media sites by the School will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the headteacher.
- Official school social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- Staff will use school provided email addresses to register for and manage official school approved social media channels.
- Members of staff running official school social media channels will sign a specific AUP to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official school social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official school social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use by the School will be in line with existing policies including anti-bullying and child protection.
- Images or videos of children will only be shared on official school social media sites/channels in accordance with the School's Photographic Image Use Policy.
- Information about safe and responsible use of school social media channels will be communicated clearly and regularly to all members of the school community.
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the school website and take place with written approval from SLT.
- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency such as staff absence.
- Parents/Carers and students will be informed of any official school social media use, along with expectations for safe use and school action taken to safeguard the community.

3.3 Staff official use of social media

- If members of staff are participating in online activity as part of their capacity as an employee of the School, then they are requested to be professional at all times and that they are an ambassador for the School.
- Staff using social media officially will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the School.

- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within school, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any image posted on the School's social media channel have appropriate written parental consent.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
- Staff using social media officially will inform their line manager, the School's online safety (e-Safety) lead and/or the head teacher of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with students or parents/carers through social media and should communicate via school communication channels.
- Staff using social media officially will sign the School's social media AUP before official social media use will take place.

3.4 Staff personal use of social media

- Personal use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the School's AUP.
- All members of staff are advised not to communicate with or add as 'friends' any current or past students or current or past students' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with line manager/ member of SLT/ Headteacher.
- If ongoing contact with students is required once they have left the School's roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- All communication between staff and members of the School community on school business will take place via official approved communication channels (*such as school email address or phone numbers*). Staff must not use personal accounts or information to make contact with students or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
- Any communication from students/parents received on personal social media accounts will be reported to the School's DSL.
- Information staff members have access to as part of their employment, including photos and personal information about students and their family members, colleagues etc. will not be shared or discussed on personal social media sites.

- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and should ensure that their social media use is compatible with their professional role, in accordance with the School's policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify SLT immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the School.
- Members of staff are encouraged not to identify themselves as employees of the School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider school community.
- Members of staff will ensure that they do not represent their personal views as that of the School on social media.
- School email addresses will not be used for setting up personal social media accounts.
- Members of staff who follow/like the School's social media channels will be advised to use dedicated professionals accounts where possible to avoid blurring professional boundaries.

3.5 Students use of social media

- Safe and responsible use of social media sites will be outlined for students and their parents as part of the School's AUP.
- Personal publishing on social media sites will be taught to students as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
- Students will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, information through photographs, email addresses, full names of friends/family, specific interests and clubs etc.
- Students will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Students will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Parents will be informed of any official social media use with students and written parental consent will be obtained, as required.

- Any official social media activity involving students will be moderated by the School where possible.
- Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of the School community to take steps to ensure that mobile phones and personal devices are used responsibly.
- The use of mobile phones and other personal devices by young people and adults will be decided by the School and covered in appropriate policies including the School's AUP.
- The School recognises that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents/carers but requires that such technologies need to be used safely and appropriately within school.

4.2 Expectations for safe use of personal devices and mobile phones

- Electronic devices of all kinds that are brought in to the School are the responsibility of the user at all times. The School accepts no responsibility for the loss, theft or damage of such items. Nor will the School accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the School community and any breaches will be dealt with as part of the School discipline/behaviour policy.
- Members of staff will be issued with a school/work phone number and email address where contact with students or parents/carers is required.
- All members of the School community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of the School community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
- All members of the School community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the School's policies.
- School mobile phones and devices must always be used in accordance with the AUP
- School mobile phones and devices used for communication with parents and students must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

4.3 Students use of personal devices and mobile phones

- Students will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- All use of mobile phones and personal devices by students will take place in accordance with the Acceptable Use Policy.
- Mobile phones and personal devices will be switched off and kept out of sight during classroom lessons and while moving between lessons.
- Mobile phones or personal devices will not be used by students during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff. The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
- If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity then it will only take place when approved by SLT.
- If a student needs to contact his/her parents/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. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the Headteacher.
- 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 personal devices and will be made aware of boundaries and consequences.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone or personal 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.
- If a student breaches the School's 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/carers in accordance with the school policy.
- School staff may confiscate a student's mobile phone or device if they believe it is being used to contravene the School's behaviour or bullying policy. The phone or device may be searched by a member of SLT with the consent of the student or parent/carer. Searches of mobile phone or personal devices will be carried out in accordance with the Schools policy.
- If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

4.5 Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the School in a professional capacity. Any pre-existing relationships which could compromise this must be discussed with leaders/managers.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.

- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
- Bluetooth or other forms of communication should be switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of SLT in emergency circumstances.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the School policy then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted and allegations will be responding to following the allegations management policy.

4.6 Visitors use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the schools policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the School's Photographic Image Use Policy.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the DSL of any breaches of use by visitors.

5 Policy Decisions

5.1. Reducing online risks

- The School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit and the School's Senior Leadership Team (SLT) will ensure that appropriate risk assessments are carried out before use in school is allowed.

    - The School will ensure that appropriate filtering systems are in place to prevent staff and students from accessing unsuitable or illegal content.
    - Our Imprero server will
        - Inspect everything that is typed or done
        - Will take screen shots and will report any suspicious use detected
        - Detect when proxy bypass sites have been used
        - Help stop downloads of obscene or offensive content
        - Potentially get an early warning of predator grooming
        - Can help warn when pupils are planning to meet people they don't know
        - Help pick up 'cries for help' helping to:
            - Reduce fears over suicide, self-harm and abuse
            - Take appropriate action quickly
            - Strengthen your pastoral care

- The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer or device.
- The School will audit technology use to establish if the Online Safety (e–Safety) Policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by SLT.
- Filtering decisions, internet access and device use by students and staff will be reviewed regularly by SLT.

5.2. Internet use throughout the wider school community

- The School will liaise with local organisations to establish a common approach to online safety (e–Safety).
- The School will provide an AUP for any guest/visitor who needs to access the School computer system or internet on site.

5.3 Authorising internet access

- The School will maintain a current record of all staff and students who are granted access to the School's electronic communications.
- All staff, students and visitors will read and sign the School's AUP before using any school ICT resources.
- Parents will be informed that students will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the School's AUP for student access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the School community (such as with children with special education needs) the School will make decisions based on the specific needs and understanding of the student(s).

6 Engagement Approaches

6.1 Engagement and education of children and young people

- An online safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst students.
- Education about safe and responsible use will precede internet access.
- Students input will be sought when writing and developing school online safety policies and practices.
- Students will be supported in reading and understanding the School's AUP in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Student instruction regarding responsible and safe use will precede Internet access.
- Online safety (e-Safety) will be included in the PSHCE, and computing programmes of study covering both safe school and home use.

- The student Acceptable Use expectations and Posters will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the School's internal online safety (e-Safety) education approaches.
- The School will reward positive use of technology by students.
- The School will implement peer education to develop online safety as appropriate to the needs of the students.

6.2 Engagement and education of children and young people who are considered to be vulnerable

- The School is aware that some children may be considered to be more vulnerable online due to a range of factors and will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. AENCO).

6.3 Engagement and education of staff

- The Online Safety (e-Safety) Policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of school safeguarding practice.
- To protect all staff and students, the School will implement AUP which highlights appropriate online conduct and communication.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.
- Members of staff with a responsibility for managing filtering systems or monitor ICT use will be supervised by SLT and will have clear procedures for reporting issues or concerns.
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the students.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

6.4 Engagement and education of parents and carers

- The School recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the School's Online Safety (e-Safety) Policy and expectations in newsletters, letters, the school prospectus and on the school website.

- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, and sports days.
- Parents will be encouraged to read the School's AUP for students and discuss its implications with their children.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.

7. Managing Information Systems

7.1 Managing personal data online

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

7.2 Security and Management of Information Systems

- The security of the School Information Systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the School's network will be regularly checked.
- The computing coordinator/network manager will review system capacity regularly.
- The appropriate use of user logins and passwords to access the school network will be enforced for all but the youngest users.
- All users will be expected to log off or lock their screens/devices if systems are unattended.
- The School will log and record internet use on all school owned devices.

Password policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and students must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
- All students are provided with their own unique username and private passwords to access school systems. Students are responsible for keeping their password private.

- We require staff and students to use STRONG passwords for access into our system.

7.3 Filtering Decisions

- The School's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our students, with advice from technical, educational and safeguarding staff.
- The School uses educational filtered secure broadband connectivity through the KPSN which is appropriate to the age and requirement of our students.
- The School uses Light Speed filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- The School will ensure that age and ability appropriate filtering is in place whilst using school devices and systems to try and prevent staff and students from being accidentally or deliberately exposed to unsuitable content.
- The School will work with EIS and the Schools Broadband team or broadband/filtering provider to ensure that filtering policy is continually reviewed.
- The School will have a clear procedure for reporting breaches of filtering which all members of the School community (all staff and all students) will be made aware of.
- If staff or students discover unsuitable sites, the URL will be reported to the School DSL and will then be recorded and escalated as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the School's filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from SLT.
- All changes to the School's filtering policy will be logged and recorded.
- SLT will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the School believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP immediately.

7.4 Management of applications (apps) used to record children's progress

- The Headteacher is ultimately responsible for the security of any data or images held of children.
- Apps/systems which store personal data will be risk assessed prior to use.
- Personal staff mobile phones or devices will not be used for any apps which record and store children's personal details, attainment or photographs.
- Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs.
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
- Staff and parents/carers will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.

8. Responding to Online Incidents and Concerns

- All members of the School community will be informed about the procedure for reporting online safety (e-Safety) concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
- The DSL will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Complaints about online bullying will be dealt with under the School's Anti-bullying Policy and procedure
- Any complaint about staff misuse will be referred to the Headteacher
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Students, parents and staff will be informed of the School's complaints procedure.
- Staff will be informed of the Complaints and Whistleblowing Procedures.
- All members of the School community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The School will manage online safety (e-Safety) incidents in accordance with the school discipline/behaviour policy where appropriate.
- The School will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the School will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the School will contact the Education Safeguarding Team or Kent Police via 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.
- If the School is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the Education Safeguarding Team to communicate to other schools/settings in Kent.
- Parents and children will need to work in partnership with the school to resolve issues.

Appendix A

9 Procedures for Responding to Specific Online Incidents or Concerns

9.1 Responding to concerns regarding Self-Generated Indecent Images of Children (SGIIOC or "Sexting")

- The School ensures that all members of the community are made aware of the social, psychological and criminal consequences of sharing, possessing and creating indecent images of children (known as "sexting").
- The School will implement preventative approaches via a range of age and ability appropriate educational approaches for students, staff and parents/carers.
- The School views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the DSL.
- If the School is made aware of incident involving indecent images of a child the School will:
  - Act in accordance with the School's Child Protection and Safeguarding Policy and the relevant Kent Safeguarding Child Boards procedures.
  - Immediately notify the Designated Safeguarding Lead.
  - Store the device securely.
  - Carry out a risk assessment in relation to the children(s) involved.
  - Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
  - Make a referral to children's social care and/or the police (as needed/appropriate).
  - Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
  - Inform parents/carers about the incident and how it is being managed.
  - Implement appropriate sanctions in accordance with the School's Behaviour Policy but taking care not to further traumatise victims where possible.
  - Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.
- The School will not view the image unless there is a clear need or reason to do so.
- The School will not send, share or save indecent images of children and will not allow or request children to do so.
- If an indecent image has been taken or shared on the school/settings network or devices then the School will take action to block access to all users and isolate the image.
- The School will need to involve or consult the police if images are considered to be illegal.
- The School will take action regarding indecent images, regardless of the use of school equipment or personal equipment, both on and off the premises.
- The School will follow the guidance (including the decision making flow chart and risk assessment template) as set out in "'Sexting' in schools: advice and support around self-generated images. What to do and how to handle it".
- The School will ensure that all members of the community are aware of sources of support.

9.2. Responding to concerns regarding Online Child Sexual Abuse

- The School will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The School will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for students, staff and parents/carers.
- The School's views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the DSL.
- If the School is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- If the school is made aware of incident involving online child sexual abuse of a child then the School will:
  - Act in accordance with the School's Child Protection and Safeguarding Policy and the relevant Kent Safeguarding Child Boards procedures.
  - Immediately notify the DSL.
  - Store any devices involved securely.
  - Immediately inform Kent police via 101 (using 999 if a child is at immediate risk) or alternatively to CEOP by using the Click CEOP report form: http://www.ceop.police.uk/safety-centre/
  - Where appropriate the School will involve and empower children to report concerns regarding online child sexual abuse.
  - Carry out a risk assessment which considers any vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies).
  - Make a referral to children's social care (if needed/appropriate).
  - Put the necessary safeguards in place for student(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
  - Inform parents/carers about the incident and how it is being managed.
  - Review the handling of any incidents to ensure that the school is implementing best practice and the School's SLT will review and update any management procedures where necessary.
- The School will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
- The School will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If students at other schools are believed to have been targeted then the School will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.
- The School will ensure that the Click CEOP report button is visible and available to students and other members of the school community, for example including the CEOP report button on the school website homepage and on intranet systems.

9.3. Responding to concerns regarding Indecent Images of Children (IIOC)

- The School will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- The School will take action regarding IIOC regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will take action to prevent access accidental access to IIOC for example using an Internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- If the School is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- If the school/setting are made aware of IIOC then the School will:
  - Act in accordance with the School's Child Protection and Safeguarding Policy and the relevant Kent Safeguarding Child Boards procedures.
  - Immediately notify the School's DSL.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), Kent police via 101 (using 999 if a child is at immediate risk) and/or the Local Authority Designated Office (LADO) (if there is an allegation against a member of staff).
- If the school are made aware that a member of staff or a student has been inadvertently exposed to IIOC whilst using the internet then the School will:
  - Ensure that the DSL lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
- If the School are made aware that IIOC have been found on the School's electronic devices then the school will:
  - Ensure that the DSL is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- If the School are made aware that a member of staff is found in possession of IIOC on their electronic device provided by the School, then the School will:
  - Ensure that the DSL is informed or another member of staff in accordance with the School's whistleblowing procedure.
  - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
  - Inform the LADO and other relevant organisations in accordance with the schools managing allegations policy.
  - Follow the appropriate school policies regarding conduct.

9.4. Responding to concerns regarding radicalisation or extremism online

- The School will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school and that suitable filtering is in place which takes into account the needs of students.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the DSL will be informed immediately and action will be taken in line with the School's Safeguarding Policy.

9.5. Responding to concerns regarding cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of the School's community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.
- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
- If the school is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The School will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Students, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools e-Safety ethos.
- Sanctions for those involved in online or cyberbullying may include:
  - Those involved will be asked to remove any material deemed to be inappropriate or offensive.
  - A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
  - Internet access may be suspended at school for the user for a period of time. Other sanctions for students and staff may also be used in accordance to the schools anti-bullying, behaviour policy or AUP.
  - Parent/carers of students involved in online bullying will be informed.
  - The Police will be contacted if a criminal offence is suspected.

Student & Parent Acceptable Use Policy

At Walderslade Girls' School we want to ensure that all members of our community are safe and responsible users of technology.

We will support students to:

- Become empowered and responsible digital creators and users
- Use our school resources and technology safely, carefully and responsibly
- Be kind online and help us to create a school community that is respectful and caring, on and offline
- Be safe and be sensible online and always know that you can talk to a trusted adult if you need help.

Acceptable Use Policy for all Students

- I know that school computers and Internet access has been provided to help me with my learning and that other use of technology may not be allowed. If I'm not sure if something is allowed then I will ask a member of staff
- I know that my use of school computers and Internet access will be monitored
- I will keep my password safe and private as my privacy, school work and safety must be protected
- I will write emails and online messages carefully and politely; as I know they could be forwarded or seen by someone I did not intend
- I know that people I meet online may not be who they say they are. If someone online suggests meeting up then I will immediately talk to an adult and will always arrange to meet in a public place, with a trusted adult present
- I know that bullying in any form (on and offline) is not tolerated and I know that technology should not be used for harassment
- I will not deliberately upload or add any images, videos, sounds or text that could upset, threaten the safety of or offend any member of the school community
- I understand that it may be a criminal offence or breach of the school policy to download or share inappropriate pictures, videos or other material online. I also understand that it is against the law to take, save or send indecent images of anyone under the age of 18 and will visit www.thinkuknow.co.uk
- I will protect my personal information online at all times
- I will not access or change other people files, accounts or information
- I will only upload appropriate pictures or videos of others online and when I have permission
- I will only use my personal device/mobile phone in school if I have permission from a teacher
- I will respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources
- I will always check that any information I use online is reliable and accurate
- I will make sure that my internet use is safe and legal and I am aware that online actions have offline consequences
- I will only change the settings on the computer if a teacher/technician has allowed me to

- I know that use of the school's ICT system for personal financial gain, gambling, political purposes or advertising is not allowed
- I understand that the school's Internet filter is there to protect me, and I will not try to bypass it
- I know that if the school suspect that I am behaving inappropriately with technology, then enhanced monitoring and procedures may be used, such as checking and/or confiscating personal technologies such as mobile phones and other devices
- I know that if I do not follow the Acceptable Use Policy then I may lose privileges in line with the school Behaviour Policy.
- If I am aware of anyone trying to misuse technology then I will report it to a member of staff
- I will speak to an adult I trust if something happens to either myself or another student which makes me feel worried, scared or uncomfortable
- I will visit www.thinkuknow.co.uk www.childnet.com and www.childline.org.uk to find out more about keeping safe online
- I have read and talked about these rules with my parents/carers

Parent/Carers Acceptable Use Policy

- I have read and discussed the Acceptable Use Policy with my child
- I know that my child will receive online safety (e-Safety) education to help them understand the importance of safe use of technology and the internet, both in and out of school
- I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons and to safeguard both my child and the school's systems. This monitoring will take place in accordance with data protection and human rights legislation
- I understand that the school will take all reasonable precautions to ensure that students cannot access inappropriate materials but I appreciate that this is a difficult task. I understand that the school cannot be held responsible for the content of materials accessed through the Internet and the school is not liable for any damages arising from use of the Internet facilities
- I understand that if the school has any concerns about my child's safety online, either at school or at home, then I will be contacted
- I understand that if my child does not abide by the school's Acceptable Use Policy then sanctions will be applied in line with the school's Behaviour and Anti-bullying Policy. If the school believes that my child has committed a criminal offence then the Police will be contacted
- I, together with my child, will support the school's approach to online safety (e-Safety) and will not deliberately upload or add any images, videos, sounds or text that could upset, threaten the safety of or offend any member of the school community
- I know that I can speak to the school Online Safety (e-Safety) Coordinator (Ms Ranson), my child's teacher or the Headteacher if I have any concerns about online safety (e-Safety)
- I will visit the school website for more information about the school's approach to online safety as well as to access useful links to support both myself and my child in keeping safe online at home
- I will visit www.thinkuknow.co.uk/parents, www.nspcc.org.uk/onlinesafety, www.internetmatters.org www.saferinternet.org.uk and www.childnet.com for more information about keeping my child(ren) safe online
- I will support the school and my child by role modelling safe and positive online behaviour (such as sharing images, text and video responsibly) and by discussing online safety with them when they access technology at home.

Staff Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using ICT and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites.

2. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

4. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly).

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the Network Manager.

6. I will ensure that any personal data of students, staff or parents/carers is kept in accordance with the Data Protection Act 1998. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school). Any images or videos of students will only be used as stated in the school's Photographic Image Use Policy and will always take into account parental consent.

7. I will not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, tablets, digital cameras, mobile phones), unless they are suitably secured and encrypted. Where possible I will use the Home Access Plus to upload any work documents and files in a password protected environment). I will protect the devices in my care from unapproved access or theft.

8. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

9. I will respect copyright and intellectual property rights.

10. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of students within the classroom and other working spaces

11. I will report all incidents of concern regarding children's online safety to a member of the Safeguarding Team or the Online Safety Coordinator (Emma Ranson) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to a member of the Safeguarding Team or the Online Safety Coordinator as soon as possible.

12. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the Network Manager as soon as possible.

13. My electronic communications with students, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Headteacher.

14. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.

15. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, into disrepute.

16. I will promote online safety with the students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

17. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with a member of the Safeguarding Team or the Online Safety Coordinator (Emma Ranson) or the Headteacher.

18. I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

Visitor / Volunteer Acceptable Use Policy

This Acceptable Use Policy may also be useful for staff who do not access school ICT systems

As a professional organisation with responsibility for children's safeguarding it is important that all members of the community are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy. This is not an exhaustive list and visitors/volunteers are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I will ensure that any personal data of students, staff or parents/carers is kept in accordance with the Data Protection Act 1998. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of students will only be used as stated in the school image use policy and will always take into account parental consent.

2. I have read and understood the school's Online Safety (e-Safety) Policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of students within the classroom and other working spaces.

3. I will follow the school's policy regarding confidentially, data protection and use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

4. My electronic communications with students, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership Team and/or Headteacher.

5. My use of ICT and information systems will be compatible with my role within school. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. I will take appropriate steps to protect myself online and my use of ICT will not interfere with my work duties and will always be in accordance with the school AUP and the Law

6. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or into disrepute.

7. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

8. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead (Ms E Ranson) or the Headteacher.

9. I will report any incidents of concern regarding children's online safety to a member of the Safeguarding Team as soon as possible.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

WiFi Acceptable Use Policy

For those using school WiFi

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the school's boundaries and requirements when using the school WiFi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. This is not an exhaustive list and all members of the school community are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

Please be aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The school takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the school premises that is not the property of the school.

The school provides WiFi for the school community and allows access for educational use only. Access to the WiFi is granted at the IT team's discretion. Once connected you will be prompted to login to the internet with your standard network account details. All wireless/internet access is monitored to maintain the school's standards of the acceptable use policy.

1. The use of ICT devices falls under Walderslade Girls' School's Acceptable Use Policy, Online Safety (e-Safety) Policy and Behaviour Policy) which all students/staff/visitors and volunteers must agree to, and comply with.

2. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

3. School owned information systems, including WiFi, must be used lawfully and I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

4. I will take all practical steps necessary to make sure that any equipment connected to the school's service is adequately secure (such as up-to-date anti-virus software, systems updates).

5. The school's wireless service is secure, however the school cannot guarantee the safety of traffic across it. Use of the school's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. For that reason, I expressly agree that I knowingly assume such risk, and further agree to hold the school harmless from any claim or loss arising out of, or related to, any such instance of hacking or other unauthorised use or access into my computer or device.

6. The school accepts no responsibility for any software downloaded and/or installed, e-mail opened, or sites accessed via the school's wireless service's connection to the Internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other Internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

7. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.

8. I will respect system security and I will not disclose any password or security information that is given to me. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

9. I will not attempt to bypass any of the school's security and filtering systems or download any unauthorised software or applications.

10. My use of the school WiFi will be safe and responsible and will always be in accordance with the school AUP and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

11. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

12. I will report any online safety (e-Safety) concerns, filtering breaches or receipt of inappropriate materials to a member of the Safeguarding Team as soon as possible.

13. If I have any queries or questions regarding safe behaviour online then I will discuss them with the Online safety (e-Safety) Coordinator (Ms Ranson) or the Headteacher.

14. I understand that my use of the school's internet will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school will terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.

Social Networking Acceptable Use Policy

For parents/volunteers running school/setting social media accounts e.g. PTA groups and committees

1. As part of the school's drive to encourage safe and appropriate behaviour in the use of today's technology, I will support the school's approach to Online safety (e-Safety). I am aware that (tool using e.g. Facebook, Twitter) a public and global communication tool and that any content posted on the site/page/group may reflect on the school, its reputation and services. I will not use the site/page/group to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.

2. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school Designated Safeguarding Lead (Ms Ranson) or the Headteacher. The Headteacher (or other appropriate member of senior leadership) retains the right to remove or approve content posted on behalf of the school. Where it believes unauthorised and/or inappropriate use of the (tool using e.g. Facebook, Twitter) or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.

3. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

4. I will follow the school's policy regarding confidentially and data protection/use of images. I will ensure that I have written permission from parents/carers or the school before using any images or videos which include members of the school community. Images of students will be taken on school equipment by the school and in accordance with the school's Photographic Image Policy. Images which include students will only be uploaded by the school and these will be for the sole purpose of inclusion on (tool using e.g. Facebook, Twitter) and will not be forwarded to any other person or organisation.

5. I will promote online safety in the use of (tool using e.g. Facebook, Twitter) and will help to develop a responsible attitude to safety online and to the content that is accessed or created.

6. I will set up a specific account/profile using a school provided email address to administrate the site and I will use a strong password to secure the account. The School's Designated Safeguarding Lead and/or SLT will have full admin rights to the account.

7. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.

8. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the Designated Safeguarding Lead and/or Headteacher immediately.

9. I will ensure that the (tool using e.g. Facebook, Twitter) is moderated on a regular basis as agreed with the Designated Safeguarding Lead and/or Headteacher.

10. I have read and understood the school Online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices and the safe use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the head teacher.

11. If I have any queries or questions regarding safe and acceptable practise online I will raise them with the Designated Safeguarding Lead or the Headteacher.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.