LORDSWOOD GIRLS' SCHOOL & SIXTH FORM CENTRE

This policy is called:	Online Safety Policy
It applies to:	Lordswood Girls' School & Sixth Form Centre
Person responsible for its revision:	Assistant Headteacher (Student Behaviour, Welfare & Development)
Status:	Non-statutory, although Data Protection is statutory
Website:	Public Website
Approved by:	Governing Body
Review frequency:	Annually or more frequently if required
Date of ratification:	May 2022
Date of next review:	May 2023

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and create a context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Lordswood Girls' School's online safety policy should help to ensure safe and appropriate use.

The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher and governors to the senior leaders, middle leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

Many of the risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies such as behaviour, anti-bullying and child protection policies.

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors, supply staff, trainee teachers and 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 online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school or sixth form centre.

Lordswood Girls' School & Sixth Form Centre will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that takes place out of school.

Main Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

Individual/Groups	Main Responsibility
Governing Body	**Governors** are responsible for the approval of the Online safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing Body who will receive regular information about online safety incidents and monitoring reports.
Headteacher	**The Headteacher** is responsible for ensuring the safety (including online safety) of members of the school community and for ensuring that staff with responsibility for online safety receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant. **The Headteacher will:** ● review the school online safety policy / acceptable use of ICT and whole school ICT policy documents. ● ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place. ● meet regularly with the Network Systems & Strategic Development Manager to discuss current issues and review monitoring and filtering logs. ● Ensure that all new staff receive training in online safety as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies.
Assistant Headteacher (Learning & Achievement)	**The Assistant Headteacher (Learning & Achievement) will:-** ● have strategic oversight of the day to day online safety issues that may arise within and outside of school and review the school online safety policy / anti- bullying and behaviour documents accordingly. ● ensure that there is a system in place to allow for the reporting of online safety incidents and support those in school who carry out the internal online safety role.

	● ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place. ● receive reports of online safety incidents and ensure a log of incidents is created and updated to inform future online safety developments. ● attend Governing Body meetings to report on online safety incidences. ● receive reports of ICT/online safety incidents that contravenes the Acceptable Use Policy whist in school and ensure a log of incidents is created and updated to inform future ICT/online safety developments.
Assistant Headteacher (Learning & Achievement)	**The Assistant Headteacher (Learning & Achievement) will:-** ● provide training and advice in ICT and online safety so that staff, students and parents can together gain a better understanding of online safety issues. ● carry out an audit of online safety needs for all groups identified above regularly.
Network Systems & Strategic Development Manager	**The Network Systems & Strategic Development Manager will:-** ● have strategic oversight of the day to day ICT/online safety issues that may arise within school. ● receive regular updates through attendance at LA / other information / training sessions and by reviewing guidance documents released by LA and others. ● ensure that the school's ICT infrastructure is secure and is not open to misuse or malicious attack including servers, wireless systems and cabling. ● ensure that the school meets the online safety technical requirements outlined in the School's ICT Policy and any relevant Local Authority Online safety Policy and guidance. ● ensure that there is a system in place to allow for monitoring and filtering of ICT systems and support of those in school who carry out the internal online safety monitoring role. ● ensure that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed. A record of users and usernames will be kept and updated regularly. ● ensure that all users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded and reviewed annually. ● ensure the "master / administrator" passwords for the school ICT system are also available to the Headteacher or other nominated senior leader and kept in the school safe. ● have responsibility for the day to day filtering system in school. ● ensure that, in the event that the filtering needs to be switched off for any reason, or for any user, this is logged and reported to the Headteacher. ● ensure that requests from staff for sites to be removed from the filtered list will be considered and if agreed, this action will be recorded. ● keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

	● ensure the production / review / monitoring of the school filtering policy (if the school chooses to have one). ● take day to day responsibility for monitoring online safety practices in the use of the school network , web site, virtual learning environment ,remote access and email. ● inform the appropriate member of staff with responsibility for online safety when online safety incidences occur using school ICT systems and devices. ● meet regularly with the Headteacher to discuss current issues and review monitoring logs. ● liaise with school ICT technical staff with respect to regular monitoring and recording of user activity on the school network as well as on remote management tools. ● regularly review and carry out audits of the safety and security of school ICT systems.
Director of Intervention & Inclusion (Senior DSL)	**The Director of Intervention & Inclusion** should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:- ● sharing of personal data access to illegal / inappropriate materials ● inappropriate on-line contact with adults / strangers ● potential or actual incidents of grooming ● cyber-bullying ● radicalisation
All teaching and support staff employed at Lordswood Girls' School & Sixth Form Centre	**Teaching and support staff** are responsible for ensuring that: ● they have an up to date awareness of online safety matters and of the current school online safety policy and practices ● they have read, understood and signed the school Staff Acceptable Use Policy. ● they are responsible for the security of their username and password and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security or misuse to the Network Systems & Strategic Development Manager. ● digital communications with students (email, website, virtual learning environment) are on a professional level and only carried out using official school systems. ● online safety issues are embedded in all aspects of the curriculum and specifically in ICT and PSHE whereby current practices and technologies are regularly reviewed. ● key online safety messages are reinforced in other school activities e.g. as part of a planned programme of assemblies and pastoral activities such as the morning registration programme. ● students understand and follow the school online safety and acceptable use policy and are encouraged to adopt safe and responsible use of ICT, the internet and personal digital devices both within and outside school. ● students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations ● they monitor ICT activity in lessons, extra-curricular and extended school activities.

	● they are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices. ● in lessons where internet use is pre-planned students are guided to sites checked as suitable for their use and if any unsuitable material is found in internet searches this is reported to the Network Systems & Strategic Development Manager and blocked. If students are allowed to freely search the internet, staff should be vigilant in monitoring the content found. ● they act as good role models in their use of ICT, the internet and mobile devices.
All students enrolled at Lordswood Girls' School & Sixth Form Centre	**All students** are:- ● responsible for using the School ICT systems in accordance with the Student Acceptable Use Policy ● have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. ● need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. ● expected to know and understand School policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying. ● expected to understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety Policy covers their actions out of school, if related to their membership of the school.
Parents/Carers	**Parents/Carers** play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/ VLE and information about national/local online safety campaigns/ literature. Parents and carers will be responsible for:- ● endorsing the Student Acceptable Use Policy ● accessing the school websites, VLE , on-line student records in accordance with the relevant school Acceptable Use Policy.
All temporary users	**Temporary users** who access the School ICT systems / website / VLE will be expected to sign a Temporary User AUP before being provided with access to school systems.

Policy Statements

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Lordswood Girls' School & Sixth Form Centre will inform and educate users about the risks and will implement policies to reduce the likelihood of the potential for harm: -

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow the School ICT policy concerning the sharing, distribution and publication of those images. Those images should only be taken on School equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the School/Sixth Form Centre into disrepute.
- Students must not take, use, share, upload, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website - See signed media consent form and Parent Home school agreement document.
- Students' work can only be published with the permission of the student and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- Only use the encrypted USB sticks which have been issued by the school.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- **Staff and students' personal data should not be stored on any portable device, USB stick or any other removable media.**

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows Lordswood Girls' School & Sixth Form Centre currently consider the benefit of using these technologies for education outweighs their risks / disadvantages:-

	Staff & other adults				**Students (11-16)**				**Post Sixteen Students**			
Communication Technologies	**Allowed**	**Allowed at certain times**	**Allowed for selected staff**	**Not allowed**	**Allowed**	**Allowed at certain times**	**Allowed with staff discretion**	**Not allowed**	**Allowed**	**Allowed at certain times**	**Allowed with staff discretion**	**Not allowed**
Mobile phones may be brought to school	✓				✓				✓			
Use of mobile phones in lessons				✓				✓			✓	
Use of mobile phones in social time		✓						✓		✓		
Taking photos on mobile phones or other camera devices		✓					✓				✓	
Use of hand held devices eg Tablets	✓						✓				✓	

Use of personal email addresses in school, or on school network				✓				✓				✓
Use of school email for personal emails				✓				✓				✓
Use of chat rooms / facilities excluding school VLE				✓				✓				✓
Use of instant messaging excluding school VLE				✓				✓				✓
Use of social networking sites			✓				✓				✓	
Use of blogs excluding school VLE or a managed blog				✓				✓				✓

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers (email, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- All students will be provided with individual school email addresses for educational use only .
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Sanctions

Incident	Who should deal with it?	Level of sanction/response?	Who should it be referred to?
Inappropriate use of Mobile phones in lesson/in school e.g. taking photos and/or filming without consent, accepting messages or partaking in live chat, sexting	All staff	It is the student's responsibility to ensure their phone is not seen on site, they should hand them in at the start of the day to student reception or lock them away in their lockers. If a phone is seen anywhere on school site it will be confiscated. If it is a first offence the student will not be able to have the phone back until the end of the day. If it is a second offence the student will not be able to have	Intervention & Behaviour Support Manager. If a sixth form student Assistant Director Post-16 Studies

		the phone back for 24 hours (the end of the following school day). If it is a third offence the student will not be able to have the phone back for 3 school days. The fourth offence will result in the student receiving a day in internal exclusion and will be required to hand their phone in to reception every morning for. Students who hand in their phones are able to collect it at the end of the day. Should the second or third offence coincide with a school holiday or weekend and the parents wish their child to have their phone, the parent/carer must collect the phone before 4pm on the final day before that holiday/weekend and the phone must be returned by parents on the first school day back for the sanction to be fulfilled.	If refusal to hand over mobile phone then refer to a member of SLT DSL (for safeguarding concerns e.g. sexting)
Inappropriate use of hand held devices e.g. Tablets	All staff	Tablet confiscated for 1 day. Alert slip issued and a detention set by the teacher. Confiscated tablet handed to reception. Collected at end of the day. Subsequent confiscations are kept for a period of one week. Tablet must be collected by a parent/guardian.	Intervention & Behaviour Support Manager. If refusal to hand over mobile phone then refer to a member of SLT DSL (for safeguarding concerns)
Inappropriate use of School IT systems/the Internet, e.g. searching for inappropriate content, downloading illegal materials, inappropriate use of social media and downloading illegal materials pertaining to radicalisation	All staff	Alert slip and a detention. Internet access disabled for up to 2 weeks depending on the severity of the incident. 1 -3 days isolation meeting with Parents/Guardian Meeting with Parents/Guardian and/or Police Office responsible for PREVENT.	Intervention & Behaviour Support Manager. Assistant Headteacher (Student Behaviour, Welfare & Development) DSL (for safeguarding concerns)
Misuse of School email during a lesson	All staff	Alert slip and a detention. Email access disabled for up to 2 weeks depending on the severity of the incident. 1 -3 days isolation	Intervention & Behaviour Support Manager.

		Meeting with Parents /Guardian	
Use of school IT system to bully , harass and intimidate (including racist incidents)	All staff	IT system access disabled for up to 2 weeks Meeting with parents and/or Police Community Liaison officer 1-3 days isolation according to severity of incident or in extreme cases exclusion.	Intervention & Behaviour Support Manager. Achievement Co-ordinator/ Assistant Headteacher (Student Behaviour, Welfare & Development)
Plagiarism/ copyright breach	All staff	IT system access disabled for up to 2 weeks 1 day isolation plus work resubmitted.	Intervention & Behaviour Support Manager. Assessment & Data Manager Assistant Headteacher (Curriculum & Assessment)
Serious abuse of ICT facilities / Internet User Agreement e.g. Hacking of school network	All staff	IT systems access disabled for up to 2 weeks 1-3 days isolation according to severity of incident or in extreme cases exclusion.	Assistant Headteacher (Student Behaviour, Welfare & Development) Network Systems & Strategic Development Manager Headteacher

Monitoring

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys/questionnaires of
  - students / pupils (eg Ofsted “Tell-us” survey / CEOP ThinkUknow survey)
  - parents / carers
  - staff

Schedule for Monitoring

The implementation of this online safety policy will be monitored by the:	Senior Leadership team and Safeguarding Link Governor
The Governing Body will receive a termly report on the implementation of the online safety policy (which will include anonymous details of online safety incidents):	Governing Body
The Online safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of	Senior Leadership Team

the technologies, new threats to online safety or incidents that have taken place:	
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Police/LADO/CASS

Links to other school policies

This policy should be used in conjunction with the following whole school policies:-

ICT policy: https://drive.google.com/file/d/1_NCbhPdCDRZ4pyaopP-wX6jvyGwDZlCa/view
Anti-bullying policy: https://drive.google.com/file/d/17GU3mcuhQYmKw6cff4NC7neeSpWF3sEv/view
Disciplinary policy: https://drive.google.com/file/d/15l-n6pHzMyU6oWjjvBOc3hpKhfHBXw1R/view
Safeguarding & Child Protection policy:
https://drive.google.com/file/d/1DCHOVRuqshM1tHwyAJJOATAiYfHBm7iO/view
Staff Code of Conduct: https://drive.google.com/file/d/10izRYwhB6-VL65XNaOaxU7Z4pPr0ka9o/view