Herts for Learning

Katherine Warington School

Online/eSafety Policy

2018/19

Contents

1. Introduction

Katherine Warington School recognises that internet, mobile and digital technologies provide a good opportunity for children and young people to learn, socialise and play, provided they are safe. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that all students, staff and governors will be able to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some students may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in the safeguarding of children.

2. Responsibilities

The headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online Safety Co-ordinator in this school is Tony Smith.

All breaches of this policy must be reported to Tony Smith.

All breaches of this policy that may have put a child at risk must also be reported to the DSL.

If any organisation is hiring the school facilities and has any access to the school network and equipment, then they must adhere to the school's online safety procedures and Acceptable Use agreements.

3. Scope of policy

The policy applies to:

- students
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that students who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its Acceptable Use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: Safeguarding, GDPR, Health and Safety, Home–School Agreement, Behaviour, and Anti-bullying policies.

4. Policy and procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for students, parents/carers, staff and governors and all other visitors to the school.

4.1. Use of email

- Staff and governors should use a school email account or approved governor communication tools for all official communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact students, parents or conduct any school business using a personal email address. Students may only use school approved accounts on the school system and only for educational purposes. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

- Staff, governors and students should not open emails or attachments from suspect sources and should report their receipt to the IT Support Team.

- Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

4.2. Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in school or before recommending them to students. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. All users must observe copyright of materials from electronic sources.

- Staff must only use pre-approved systems if creating blogs, wikis or other online areas in order to communicate with students/ families.

- When working with students, searching for images should be done through Google Safe Search (standard through the HICS service), Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative).

- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative).

- Adult material that breaches the Obscene Publications Act in the UK.

- Promoting discrimination of any kind in relation to the protected characteristics: gender identity and reassignment, gender/sex, pregnancy and maternity, race, religion, sexual orientation, age and marital status.

- Promoting hatred against any individual or group from the protected characteristics above.

- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy.

- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect.

Users must not:

- Reveal or publicise confidential or proprietary information.

- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses.

- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school.

- Use the school's hardware and Wi-Fi facilities for running a private business.

- Intimidate, threaten or cause harm to others.

- Access or interfere in any way with other users' accounts.

- Use software or hardware that has been prohibited by the school.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by a member of the SLT.

4.3. Storage of Images

- Photographs and videos provide valuable evidence of students' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).

- Photographs and images of students are only stored on the school's agreed secure networks which include some cloud based services. Staff and students may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

- Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

- Staff and other professionals working with students, must only use school equipment to record images of students where possible. If a staff member is using a Personal Device images will be transferred at the first available opportunity and deleted from the Staff member's device. An example of this is a Staff member leading a trip who would take a photo at the start of the day to provide visual evidence should it be required for further identification purposes. These photos would be deleted at the end of the day/trip whichever is sooner.

4.4. Use of personal mobile devices (including phones)

- The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of students. Under no circumstance does the school allow a member of staff to contact a student or parent/carer using their personal device.

- Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

- Students are allowed to bring personal mobile devices/phones to school but may only use them in School in line with the School's Bring Your Own Device (BYOD) Policy which prevents use outside of lessons. Devices may only be used in lessons at the discretion of the Classroom Teacher.

- The school is not responsible for the loss, damage or theft on school premises of any personal mobile device.

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

- Personal Mobile devices can be used to access school emails however in the event of the devices being lost/stolen this should be reported to the DPO at the earliest opportunity. There are systems in place to remove school emails from personal devices. Personal devices used to access should be protected with Anti-Virus software and a password as a minimum.

4.5. New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, students and staff should not assume that new technological devices will be allowed in school and should check with the IT Support Team before they are brought into school.

4.6. Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a student or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs, the student or adult must report the incident immediately to the first available member of staff, the DSL or the headteacher. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.

5. Curriculum

Online safety is embedded within our curriculum. The school provides a comprehensive curriculum for online safety which enables students to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for students to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Students are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity.

- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment.

- Developing critical thinking skills in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives).

- Understanding the dangers of giving out personal details online (e.g. full name, address, mobile/home phone numbers, school details, IM/email address) and the importance of maintaining maximum privacy online.

- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others.

- Understanding the permanency of all online postings and conversations.

- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.

- What constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

6. Staff and governor training

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with students.

Any organisation working with children based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement (Appendix B).

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (Appendix B).

7. Working in partnership with parents/carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website and our Newsletter.

Students are asked on a termly basis to read and sign the Acceptable Use Agreement. A summary of key parent/carer responsibilities will also be provided and is available in Appendix A. The Acceptable Use Agreement explains the school's expectations and student and parent/carer responsibilities. The support of parents/carers is essential to implement the online safety policy effectively and keep all children safe.

8. Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to

students and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported.

The school supports students and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

9. IT Acceptable Use policies

Katherine Warington School has 3 IT Acceptable use Policies – One for Staff & Visitors, One for Students and One for Governors. The Staff Policy is available on the Staff Shared Area and is also accepted termly on screen. The Student Policy is available on the School Website and is also accepted termly on screen by Students. The Governor Policy is available from the Clerk to the Governors and is available on the Governors Shared Area.

10. Social Media – Twitter/Facebook/Instagram Guidelines

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Our school uses Facebook and Twitter to communicate with parents and carers.
- The Network Manager is responsible for the KWS postings on these technologies and monitors responses from others.
- Staff are able to setup KWS Twitter in accordance with school guidelines.
- Students are not permitted to access their social media accounts whilst at school
- Staff, governors, students, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, governors, students, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff, governors, students, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

10.1. Twitter Guidelines

Twitter is a 'micro blogging' platform which allows users to post short text messages (up to 280 characters in length). Twitter also allows for the attachment of photos and the embedding of links to other web pages.

<u>Twitter: Departmental use Guidelines</u>

- Students and Parents/Guardians should be encouraged to follow

@KWS[Department]. E.g. KWSICT

- Information regarding special achievements will be published as will other Departmental information such as fixtures and results for the PE Department.
- Changes to the extra-curricular timetable will be published as a matter of urgency.
- Specific students will only be mentioned if they have opted to follow an KWS Departmental Twitter account.
- Mentions of specific students will only be made using their Twitter ID.
- Photographs of students will only be used if permission has been granted by a Parent/Guardian and the department account is followed by the student in question and full names will not be mentioned with the photographs.
- Links to interesting articles will be tweeted in order to help develop literacy and enhance learning opportunities.
- A wide range of academic bodies and personalities connected to the academic world will be followed to help widen our students' academic horizons and to promote positive role models.
- Open tweets from followers may be replied to and positive debate encouraged.
- Students and Parents/Guardians will not be 'followed' by the ANY Departmental account.
- The Twitter feed will not be used to send 'direct messages'.
- Students will not be allowed to follow staff member's personal accounts.
- Despite encouraging debate - political views, comments and opinions will be avoided.
- School staff will not tweet any Departmental Twitter account from their personal Twitter accounts.
- Due care and consideration must be taken before sending any tweet. Content should only be tweeted if appropriate for a classroom environment.
- In the interests of safeguarding, all accounts will be overseen by the school's Senior Leadership Team.

Twitter Guidelines: Student/Parent/Carer Use

Followers of @KWS[Department] must read and abide by the terms of this document. Any student that does not comply with the acceptable use policy will be blocked and may be reprimanded in line with the school behaviour policy.

Followers must not abuse this communication facility in any way. This includes sending tweets that may be offensive to others.

Any follower sending inappropriate tweets will be blocked immediately.

Followers must not send 'direct messages' to @KWS[Department].

Followers may tweet or reply to @KWS[Department] but must understand that a reply may not always be received.

Followers must not apply to follow staff members' private accounts.

All members of the Katherine Warington School community are encouraged to follow the school accounts.

Only children over the age of 13 should have access to twitter.

The School expects students to adhere to their parents' wishes regarding their use of twitter.

10.2. Facebook Guidelines

Facebook is an online social media networking service. Registered users can then like pages to find out information about businesses/services and become friends with people they know in order to view their profile. Facebook also allows for the attachment of photos and the embedding of links to other web pages. The main difference between Facebook and email/SMS messaging is that conversations take place in the open rather than in private. This allows for messages to be aimed at a large audience. The Social media platform is experiencing a phenomenal adoption curve in the UK and being used increasingly by government departments, news agencies, commercial companies and schools, as well as individuals. It is free to use, can be used in a short space of time and has the potential to deliver many benefits in support of our communication objectives. Any information posted on Facebook will also be available on the School website and School twitter feed..

<u>Facebook: Usage Guidelines</u>

- Students and Parents/Guardians should be encourged to like the School's Facebook page.
- Information regarding special achievements will be published as will other Departmental information such as fixtures and results for the PE Department.
- Changes to the extra-curricular timetable will be published as a matter of urgency.
- No students will be mentioned by name.
- Photographs of students will only be used if permission has been granted by a Parent/Guardian.
- The Facebook page will not be used to send 'private messages'.
- Students will not be allowed to add staff member's personal accounts.

- Political views, comments and opinions will be avoided.

- In the interests of safeguarding, the schools Facebook page will be overseen by the school's Senior Leadership Team.

Facebook: Student/Parent/Carer Use

- Individuals who 'like' the schools Facebook page must read and abide by the terms of this document. Any student that does not comply with the acceptable use policy will be blocked and may be reprimanded in line with the school behaviour policy.

- Individuals must not abuse this communication facility in any way. This includes sending messages or comments that may be offensive to others.

- Any individual sending inappropriate messages or comments will be blocked immediately.

- Individuals must not send 'Private messages' to Katherine Warington School

- Individuals may comment on posts by Katherine Warington School but must understand that no replies will be forthcoming.

- Individuals must not apply to be friends with staff members' personal accounts.

- All members of the Katherine Warington School community are encouraged to like the schools Facebook page.

- Only children over the age of 13 should have access to Facebook.

- The School expects students to adhere to their parents' wishes regarding their use of Facebook.

10.3. Instagram Guidelines

Instagram is an online photo sharing application. Registered users can then like profiles to view images posted by that Profile. Instagram is a fast growing photo sharing platform and is now used by most teenagers as the most popular way of sharing images.

Instagram: Usage Guidelines

- Students and Parents/Guardians should be encouraged to like the School's Instagram profiles.

- Information regarding special achievements will be published as will other Departmental successes such as results for the PE Department.

- No students will be mentioned by name.

- Photographs of students will only be used if permission has been granted by a Parent/Guardian.

- The Instagram page will not be used to send ‘private messages’.

- Students will not be allowed to follow staff member’s personal profiles.

- Political views, comments and opinions will be avoided.

- In the interests of safeguarding, the school’s Instagram page will be overseen by the school’s Senior Leadership Team.

Instagram: Student/Parent/Guardian Use

- Individuals who ‘like’ the schools Instagram profiles must read and abide by the terms of this document. Any student that does not comply with the acceptable use policy will be blocked and may be reprimanded in line with the school behaviour policy.

- Individuals must not abuse this facility in any way. This includes sending messages or comments that may be offensive to others.

- Any individual sending inappropriate messages or comments will be blocked immediately.

- Individuals must not send ‘Private messages’ to Katherine Warington School

- Individuals may comment on posts by Katherine Warington School but must understand that no replies will be forthcoming.

- Individuals must not apply to be friends with staff members’ personal profiles.

- All members of the Katherine Warington School community are encouraged to like the schools Instagram profiles.

- Only children over the age of 13 should have access to Instagram.

- The School expects students to adhere to their parents’ wishes regarding their use of Instagram.

Appendix A - Online safety policy guide - Summary of key parent/carer responsibilities

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for students.

- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

- Parents/carers should not assume that students can bring technological devices to school and should always check the school policy.

- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.

- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.

- Any parent/carer, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, students and parents/carers.

Please see the full online safety policy in the policies section on the school website.

Appendix B - Guidance on the process for responding to cyberbullying incidents

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.

- Incidents should be reported immediately. Students should report to a member of staff (e.g. class teacher, headteacher) and staff members should seek support from their line manager or a senior member of staff.

- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the headteacher so that the circumstances can be recorded.

- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.

- A senior member of staff will conduct an investigation.

- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

Appendix C - Guidance for staff on preventing and responding to negative comments on social media

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy, see especially Appendix F (Online safety policy guide - Summary of key parent/carer responsibilities), clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

- Collect the facts

- As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

- If the allegations against a member of staff or a student are of a serious nature, these will need to be formally investigated. This may involve the police and the headteacher will need to follow the school's safeguarding procedures.

- If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

- Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

- Addressing negative comments and complaints

  - Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

- The meeting must:

  - Draw attention to the seriousness and impact of the actions/postings;

  - Ask for the offending remarks to be removed;

  - Explore the complainant's grievance;

  - Agree next steps;

  - Clarify the correct complaints procedures.

- If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

  - Reporting the matter to the social network site if it breaches their rules or breaks the law;

  - Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

- If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.