Queens' Federation

Online Safety Policy

Date	Actions taken	Responsible
14.06.2021	Policy updated	C Stubbs
16.05.2022	Policy ratified	Standards and Improvement Committee
19.06.2023	Policy ratified	Standards and Improvement Committee
23.09.2024	*Policy for ratification*	*Standards and Improvement Committee*
13.05.2025	Policy updated and ratified	K McIlveen C Hart

Queens' Federation Online Safety Policy

Introduction

Our pupils are growing up in an increasingly complex world, living their lives seamlessly on and off line. Use of the internet is an essential element in 21st century life for education, business and social interaction. This presents many positive and exciting opportunities, but also challenges and risks. Online safety refers to the act of staying safe online and encompasses all technological devices which have access to the internet from PCs and laptops to smartphones and tablets.

The use of technology is actively encouraged at the Queens' Federation. This comes with a responsibility to educate pupils and staff about the benefits and risks of using technology and provide safeguards and awareness enable everyone to control their online experiences.

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2020 and other statutory documents; it is designed to sit alongside the school's Safeguarding and Child Protection Policy. This policy should also be read alongside the staff and pupil Acceptable Use Policies and the AI Policy, which outline the expectations that apply to staff and pupil use of technology.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. Online safety issues can also affect adults who work or are associated with the school and this will be referenced in more detail later in this policy.

Technologies regularly used by pupils and staff include:
Staff:

- Staff laptops / iPads / desktops - staff devices can also be used at home in accordance with the staff AUP, particularly with regard to GDPR.
- Some staff have access to school systems beyond the school building (e.g. MIS systems, cloud platforms).
- Class cameras and other peripherals such as visualisers and Interactive Whiteboards
- Staff level internet access.

Pupils:

- Curriculum laptops / iPads / desktops including filtered access to the Internet and pupil level access to areas of the school network.
- Cameras and peripherals including programming resources.
- Online learning platform (e.g. Purple Mash) providing pupils with access within and beyond the school gates.

Where the school changes the use of existing technology or introduces new technologies which may pose risks to users' safety, a risk assessment will be completed to show how the risk is being mitigated and reduced to an acceptable level.

Aims

Our Federation aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology,
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the school curriculum.

Pupils in Key Stage 1 will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter whom they do not know
- The opportunities and risks arising from the use of Artificial Intelligence (AI); how to use generative AI ethically and to avoid it being misused; and the threats posed by AI

Educating Parents about Online Safety

For many parents the rapidly changing online world can be confusing and some may not feel well equipped to protect their children from its dangers. We will raise parents' awareness of online safety in letters and communications sent home or through specially arranged workshops and talks from outside providers. Information may also be sent via ParentMail if specific issues arise around a particular new form of online activity which we think parents should be aware of. On our websites, we will post information and links to online safety materials which we feel parents may find useful. Each year, we will participate in Safer Internet Day – the UK's biggest celebration of online safety – where an online issue or theme is focused on to teach pupils how to use the internet safely and responsibly. This learning will be shared with families, helping parents stay informed too.

Parents should raise queries or concerns in relation to online safety or their child's use of technology with school.

Handling Online Concerns and Incidents

It is vital that all staff recognise that online safety is a part of safeguarding as well as being part of our curriculum. Where a pupil misuses the school's ICT systems or internet we will follow the procedures set out in our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness or the specific incident. Any complaint about a staff member must be referred to the Executive Headteacher. We recognise that incidents may occur both inside and outside school. Where a member of staff becomes aware that a child may be using the internet unsafely or inappropriately outside of school, and believe it to be a safeguarding issue, they should speak to the designated safeguarding lead about the issue urgently and a decision will then be made about how to inform parents. In the event of serious misuse, the local police will be consulted in order to establish procedures for handling potentially illegal issues.

Cyber-Bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

We will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Information may be sent to parents regarding cyber-bullying to ensure they are aware of the signs, how to report it and how they can support children who may be affected.

Acceptable Use of the Internet in School

Authorising Internet Access

All internet users in school will be expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet must be for educational purposes only or for the purpose of fulfilling the duties of an individual's role.

Assessing Risks

Our school firewall (provided by the county ICT service) filters most unsuitable material in school and limits pupils' access to potentially unsafe sites. Some 'safe sites' may still contain unsafe links and due to the dual meaning of some search words, it is not possible to filter all inappropriate sites. Alongside this protection, it is important that all staff are well prepared and vigilant when using the internet with children.

Children using devices with access to the internet will be supervised at all times by at least one adult. Children will not be able to access devices during playtimes or lunchtimes except under the direct supervision of an adult. Teachers will take care when using their school laptop to share online material with children. Teachers will use the 'Safe Share' facility when sharing online material to avoid inappropriate material being viewed accidentally (safeshare.tv).

Use of Learning Platforms and Electronic Communication

Electronic communication by pupils in school will take place using a suitable learning platform, such as Purple Mash. Via this platform, children are only able to have contact with other children and staff within the school. For user security, each child will be given their own individual username and password for each platform. Children will be reminded that they should never share their password with anybody else. New pupils joining the school will be given a new password and pupils leaving the school will have their accounts deleted or frozen if required.

E-mail has the potential to become inappropriate and can lead to incidents of 'cyber-bullying' (as well as the downloading of viruses). Therefore, pupils in school will only send and receive emails via Purple Mash. Any reported incidents of 'cyber bullying' will be treated extremely seriously according to the procedures outlined in our behaviour policy. Teachers will instruct children to be cautious about what to do if they receive an upsetting email.

Access to Websites and Search Engines

Children in school only have access to sites allowed by the county firewall; sites which could potentially contain inappropriate material are disallowed. Access beyond this firewall is possible only with the permission of county, in consultation with a senior leader. This is unlikely to occur within the requirements of the primary curriculum.

However, children accessing websites still may be at risk and suitable sites must be thoroughly researched by the teachers beforehand if they are wishing to use them for teaching purposes. The same criteria should be used for websites as is used for judging the appropriateness, accuracy and reliability of books in school. However, unlike published books, there is no system of editorial checks in use on the internet, so special care will need to be taken.

Further risks pertain to the use of search engines and to children following weblinks, even from sites that the teacher has already appropriately vetted. To avoid dangers associated with mis-keying a website address,

teachers should generally use internet shortcuts saved in advance in the pupil's area of the server. Search engines (including image searches) should generally not be used by children until the Later Years, when their use will be specifically taught in order to make children aware of how to search safely and what to do if they encounter inappropriate material.

Should an unacceptable site be inadvertently accessed or a link followed, children will be regularly reminded that they should tell an adult straight away and not try to hide it out of embarrassment or fear of getting into trouble. Unsuitable sites can then be reported to the online safety officer or designated safeguarding lead who will follow Cambridgeshire County Council procedures. The online safety officer will also keep an incident log of any online issues which arise.

Should children display obsessive behaviour relating to computer games, email, websites, or chat rooms, teachers will inform senior leaders and then speak to their parent / carer.

Use of Artificial Intelligence (AI)

As outlined in the Federation's AI Policy, children will not be permitted to use AI tools directly as part of their learning in school at this time. Instead, staff will support children by teaching them about AI – what it is, where it can be found (e.g. in search engines and voice assistants), and how it is used in the world around them.

Staff are permitted to use generative AI tools (such as ChatGPT) but must adhere to the key principles set out in the AI policy.

Access to the Server

Access to the curriculum side of the server is limited to members of staff and is only possible by inputting an individual username and password. Passwords are changed every 90 days. All computers will be programmed to lock after a set time of 60 minutes if not in use. Laptops left unattended at break times should also be locked. This will be the responsibility of the class teacher. Our school database of confidential pupil data is held in SIMS via Central Hosting and requires an additional password-controlled login. This also locks after a short time, but staff are asked to be vigilant in not leaving their computers logged into Central Hosting when others might access them. Outside the school day, all teacher laptops should be locked away securely. Teachers are permitted to take their laptop off site for use at home, but are responsible for ensuring than no one other than them has access to it and that they take all reasonable steps to keep it safe and secure.

Screening of External Devices and Memory Sticks

All external devices and memory sticks brought in from outside the school should be thoroughly checked for viruses by the class teacher or IT technician before being used on a school machine. Teachers are aware of this protocol and are asked to be extra vigilant when they have visitors in the class. No electronic device (such as a phone, tablet or computer) should access the school wireless network without prior agreement by a senior leader. Any personal devices that join the school wireless network will be forced onto primary filtering as they are unknown. Only networked devices in the staff group will have staff filtering. Devices can only join the school wireless network with the wireless network key (password). Staff wanting to download any additional piece of software onto their school computer for classroom use should check with the IT technician or a senior leader before doing so.

Publishing Pupils Images and Work

The internet should be seen not only as a means of finding out information, but also as a vehicle for publishing work, giving children a sense of purpose and audience for their work. The school website provides many opportunities for this to happen, from pictures to book reviews and stories. It is natural for such work to be identified as belonging to an individual or group of pupils, but it is important that children are not easily identifiable. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website and in school literature. Permission will also be sought for photographs to be used for press purposes. An up-to-date list of photograph and website permissions will be kept in the school office and shared with staff regularly.

Children may also post photographs on our school learning platform, Purple Mash, as this can only be viewed by other school pupils and staff. Teachers will monitor this carefully to ensure it is safe and appropriate and will ensure that discussions take place about the potential risks of posting photographs on less secure social media sites. Photographs of any vulnerable children will not be posted in this way.

Use of Mobile Devices in School

Pupils are not permitted to bring mobile phones or personally owned devices into school. Pupils in Year 6 who have been given permission to walk to and from school independently must leave their mobile phone in the school office when they arrive in the morning. Pupils may collect their mobile phone from the office at the end of the school day.

The Federation accepts that employees will bring their mobile phones to work. However, school staff should not use their own mobile phone or other personal device for work in school (especially the taking of photographs). In the Early Years Foundation Stage, staff mobile phones are strictly not permitted anywhere where staff may have contact with children in fulfilment of our safeguarding towards young children.

System Security

All staff members will take appropriate steps to ensure their devices remain secure. This includes:

- Using a two factor authentication and encryption for staff laptops. Strong passwords should be at least 8 characters, with a combination of upper and lower case letters, numbers and special characters. Staff are advised to keep codes and passwords private and not to write them down.
- Encryption of the hard drive means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device. Where encryption is not enabled, we recommend sensitive data be stored on an encrypted pen drive.
- Making sure the device locks if left inactive for a period of time. The staff screensaver will activate after 90 minutes. It is the responsibility of staff to lock the laptop if leaving the device unattended.
- Not sharing the device amongst family or friends.
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date and always installing the latest updates.

Staff members must not use the device in any way which would violate the school's terms of acceptable use. Work devices must be solely used for work activities. If staff have any concerns regarding the security of their device, they must seek advice from the ICT technicians.

The pupil network login will lock after a period of 15 minutes' inactivity.

Good Practice for Staff, Pupils and Parents

Staff Personal Safety

It is vitally important that staff are careful about content that they search out or download. Every time a page is viewed on the internet, it is possible to trace the visit back to the school computer. This means that it is possible to tell if the school computer was being used to look at inappropriate web pages.

Staff must be aware of their responsibilities to the school when using social networking sites such as Facebook. Our staff code of conduct must be adhered to at all times, even outside of working hours. It is important to maintain your status as a professional teacher or member of staff of the Queens' Federation. Disciplinary action could result if the school is brought into disrepute.
While we have our own school X account (formally Twitter), we are careful about what we post and our 'Comments' settings are switched off, so that no-one can post anything inappropriate.

- Staff must not post anything on any online site that could be construed to have an adverse impact on the school's reputation.
- Staff must not post photographs related to the school on any internet site including pupils, parents, staff or the school branding e.g. school uniform.
- Staff must not form online friendships with pupils and parents.

- Staff must not post anything on a social networking site that would offend any other member of staff, pupil or parent using the school.
- All staff will attend annual online safety training.
- Staff will use their school email account for all school-related communications.
- Staff should make sure they are aware of the staff responsible for safeguarding issues.

Pupil Personal Safety

- Online safety is an important part of our school curriculum in all year groups.
- Pupils will be taught how to stay safe when working online both at school and at home.
- Pupils must not post anything on an online site that can be construed to have an adverse impact on the school's reputation.
- Pupils must not post anything on an online site that would offend any other member of staff, pupil or parents using the school.
- Pupils must not post photographs or video related to the school on any internet sites including pupils, parents, staff or the school branding e.g. school uniform.
- Pupils should never reveal their full name, address or contact details, any school user ID or password online, even if communicating with known acquaintances.
- Pupils should be aware that people can easily pose as someone else online and should employ a 'healthy mistrust' of anyone they meet 'online' unless their identity can be verified.

Parents

- Parents will be made aware of online safety in letters and communications sent home or through specially arranged workshops and talks from outside providers.
- Parents need to be aware that parental control software is often available via their ISP so that they can manage and control their child's computer and internet activity. Mobile phone operators also offer free parent control software to limit the kind of content children can access through a mobile network.
- Parents need to be aware that the parental control software does not replace the need for supervision and education when working on the internet.
- Computers for children should be used in a shared space where parents can see the screen.
- Parents should take an interest in their children's internet use and discuss various issues pertaining to the internet.
- Parents should be aware of the various age limits on games and social networking sites. These are there for a reason.
- Parents should discuss the care needed when their children meet online 'friends' and should only talk to people they know. Parents should remind their children not to give out any personal details nor details of family and friends, even to people they know. Parents should make their child aware of the dangers of meeting someone they have only met online.
- Parents should encourage their children to tell them if anything online makes them feel uncomfortable.
- Parents should be aware that they are in control and that they have every right to check on their children's online activities as well as their mobile usage.
- Parents should encourage offline activities. Socialising with friends and taking part in physical activities is really important.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues such as cyber-bullying. All staff will receive refresher training once every 3 years as part of safeguarding and child protection training, as well as relevant updates as required. The designated safeguarding lead will undertake child protection training, which will include online safety, every two years. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable.

Conclusion

In order to keep children safe, as well as to protect the reputation of our schools, it is crucial that all members of Federation staff are aware of this policy, its seriousness and the correct procedures outlined above. The Acceptable Use Policy (AUP) provides a quick-reference guide for staff who will be asked to sign it periodically

as a reminder of our policy. As use of technology in society continues to change rapidly, it is important to review these protection measures on a regular basis. This policy will be reviewed annually along with the Federation's other safeguarding policies.

The Queens' Federation aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018). This policy applies to all personal data, regardless of whether it is in paper or electronic form.

Appendix A – Queens' Federation Adult Acceptable Use Policy

This is a quick reference guide for staff regarding use of information technology inside and outside of school. It should be read in conjunction with the Federation Online Safety Policy.

School Email - Office 365

- School email should only be used for school matters.
- Personal devices configured to receive school emails should have 2 factor authentication enabled (pin / password protected device or pin / password / touch-id protected email app).
- Any attachments downloaded to personal devices from email should be deleted after use and not stored on the device.

Laptops must be:

- Locked when not in use and programmed to lock if left for extended periods.
- Kept in a secure place if left at school overnight.
- Kept safe if taken home.
- Only ever used off-site by a member of school staff to access appropriate content.

Passwords:

- Must be kept secret and not shared with other staff or supply teachers.
- Supply teachers should use the 'guest' log in.
- TAs should use their own username and password.

Using the Internet:

- Children using the internet must always be supervised.
- Children may not use computers in the classroom during wet breaktimes and lunchtimes.

Websites:

- Should be checked before lessons for appropriate content.
- Unsuitable websites should be reported to the online safety and designated safeguarding officers.
- In the event of photographs of new pupils being considered for the website, teachers will check with the office that parental permission has been given.

Viruses / Inappropriate Software:

- Memory sticks and CDs from outside of school must be checked before being used.
- No additional software (including screensavers) should be installed on a school machine without permission from the IT technicians or a senior leader.

Learning Platforms:

- Children's passwords should be kept in a secure place.
- Teachers will not use email to contact children other than for class and curriculum-based activities.
- Children will not be allowed to upload photographs of themselves or other children to their learning platform.
- Teachers will be responsible for keeping the technician up-to-date on their class register, so that learning platform accounts are current.
- Web-conferencing will always be supervised by an adult and children without photographic permission will not be allowed to take part.

Artificial Intelligence (AI):

- Children are not permitted to use AI tools in school.
- Staff must adhere to the key principles set out in the AI Policy

Social Networking Sites:

- Teachers who are members of social networking sites will not make contact with children who are currently at the school, or ex-pupils who are under the age of 18.
- Teachers will not upload any photographs containing pupils from the school.

Mobile Phones:

- Mobile phones brought in by teachers will be kept in a secure place.
- Teachers will not give out their mobile phone number to pupils.
- Children may not bring mobile phones into school or on any school trips.

Signed:_____ Name:_____ Date:_____

Appendix B – Queens' Federation Pupil Acceptable Use Policy

Pupil Acceptable Use Policy (Foundation Stage and KS1)

These rules will help us to keep everyone safe when online and using devices.

- I will ask a teacher or suitable adult if I want to use the computer or IPad.
- I will only use apps, sites or games that a teacher or suitable adult has told me to or allowed me to use.
- I will only share my passwords and log in details with my teacher, suitable adult or my parents.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets or scares me on the screen.
- I know that people online aren't always who they say they are.
- I know that anything I do online can be shared and might stay online forever.
- I will always check with my teacher, suitable adult or parents before sharing any personal information.
- I will be kind and polite to everyone, online and in person.
- I know that these rules are designed to keep me safe. If I break the rules I might not be able to use the computer or IPad and my parents may be contacted.

The school cannot accept any responsibility for access to the internet outside of school, even if the children are researching a topic related to school. We encourage all children to adhere to the rules both at school and at home.

Pupil Acceptable Use Policy (KS2)

These rules will help us to keep everyone safe when online and using devices.

- I will only use ICT systems in school, including the internet, email, digital media and mobile technologies for school purposes.
- I will ask permission from a member of staff before using the internet.
- I will not install or attempt to install programmes of any type on any school device, nor will I try to alter computer settings.
- I will only log onto the school network and school learning platforms such as Microsoft Teams, Purple Mash and Times Table Rockstars with my own user name and password.
- I will not reveal my passwords or log in details to anyone other than my parents or my teacher.
- I will only open / delete my own files and will not access other people's folders without permission.
- I will be responsible for my behaviour when using the internet. This includes the resources I access and the language I use. I will make sure that all ICT communication with other children and adults is responsible, polite and sensible.
- I will not deliberately browse, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher or my parent / carer.
- I will immediately report anything I have seen or heard online that makes me feel uncomfortable.
- I will always check with my teacher or parents before sharing any personal information.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others any distress or bring into disrepute.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I know that my parent / carer may be contacted if a member of school staff is concerned about my online safety.
- I understand that these rules are designed to keep me safe and if they are not followed (e.g. cyber-bullying, use of images or personal information) I will be subject to disciplinary action. This will include conatct with parents and , in the event of illegal activities, involvement of the police.

The school cannot accept any responsibility for access to the internet outside of school, even if the children are researching a topic related to school. We encourage all children to adhere to the rules both at school and at home.

Dear Parent / Carer,

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT. It is essential that pupils are aware of online safety and know how to stay safe when using any ICT. Many of the rules will become more relevant as the children progress through school and will have increased access to the internet and email.

Please read and discuss these e-safety rules with your child. If you would like any further information about the use of ICT in your child's year group, please speak to your child's class teacher or the school's Computing subject leader.

Please take care to ensure that appopriate systems are in place at home to protect and support your child / children.

Please return the bottom section of this form to school.

Pupil Acceptable Use Policy

We have discussed the Pupil Acceptable Use Policy and _____ (pupil's name) agrees to follow the online safety rules and support the safe use of ICT at the Queens' Federation.

Parent / Carer Signature: _____

Child Signature: _____

Class: _____

Date: _____

Please return the signed form to the school office. Thank you