QUAINTON HALL
Preparatory School & Nursery

Online Safety Policy

Owner	**SF/AR**
Updated:	**April 2021**

Policy Approved By:	**Date:**
Senior Management Team	**April 2021**
Presented and Agreed by Staff	**April 2021**
Review Date:	**January 2022**

Table of Contents

Overview

This document describes the online Safety procedures put in place within Quainton Hall School.

1. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Headmasters and school staff
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

2. Roles and responsibilities

2.1 The Governing Board

The Governing Board has overall responsibility for monitoring the online safety policy. The Governor who oversees online safety is Mr John Dunston.

2.2 The Headmaster

The Headmaster is responsible for ensuring that staff understands this policy, and that it is being implemented consistently throughout the school.

2.3 The Designated Safeguarding Lead (DSL) and Deputy DSL

The DSL (Simon Ford) and the DDSL (Ayesha Rasool) are involved if necessary following any incident involving pupils. Details of the school's DSL and DDSL's roles are set out in our Child protection and safeguarding policy as well as relevant job descriptions.

The DSL/DDSL take the responsibility for online safety in school, in particular:

- Supporting the Headmaster in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headmaster, online Safety Co-ordinator and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety. Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headmaster and/or governing board
- Keeping up to date with online safety issues which may be relevant to the school

2.4 The Online Safety Co-Ordinator – (Mike Still)

The online safety co-ordinator is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

2.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Behaviour and Discipline policy
- Understanding and using any devices in accordance with the Computer Usage and Internet Access Agreement for Staff (Appendix 3)

2.6 Parents

Parents are expected to:

- Notify a member of staff or the Headmaster of any concerns or queries regarding this policy
- Ensure they and their child has read, understood and agreed to the terms on Computer Usage and Internet Access Agreement for Pupils and adhere to the computer usage and internet access agreement (Appendix 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- https://www.childnet.com/parents-and-carers
- https://www.saferinternet.org.uk/advice-centre/parents-and-carers

3. School responsibilities

3.1 Network logins and private spaces

Pupils within PPR, PP1 and PP2 have a shared log in space for each year group, password protected. Each pupil from P3 to P8 has their own log in area, similarly password protected. Pupils and staff have access to a "public" area, into which staff and students can contribute files for distribution or for collaborative work. All members of staff have additional areas into which they can share documents among themselves, but privately from pupils. Members of the senior management team have a similarly private area. Members of staff have individual school email addresses. Pupils are not issued with school email addresses.

3.2 Physical network security

The network server is housed within the school, in its own room, with no pupil access allowed. The server room contains the server itself, the core network switching hardware and the connection to our broadband line. Other elements of the physical network are located away from pupil access. Wi-Fi hotspots are located at various points within the buildings allowing wireless connectivity for school laptops, tablets and staff devices. This connectivity is encrypted to restrict unauthorised access. Children are not permitted to have internet enabled devices with them in school. These are to be left for safe keeping in the school office during the working day.

3.3 Internet filtering

This is provided and supported by our external supplier (Core Networx), using software provided by schoolsbroadband.net. It is the responsibility of the Online Safety Co-Ordinator to regularly check filtering is up to date and enforced on the school network.

4. Educating pupils about online safety

The education of pupils in online safety is an essential part of the School's safety provision and is regularly reinforced as part of the PSCHE and ICT curriculum.

In Reception and Pre-Prep, pupils 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 from P3-P8 will be taught in addition to the school's curriculum, with the support of an external agency (most recently Childnet), to ensure the pupils;

- Use technology safely, respectfully and responsibly
- Understand the importance to keep their personal details private, including information which could identify them or their location
- Understand the responsibility of keeping themselves safe online
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact on the internet or other online technologies
- The safe use of social media and the internet will also be covered in other subjects where relevant.
- Their understanding of the Computer Usage Agreement (Appendix 1)
- How to safely use digital platforms to enhance their learning, including BOFA, MyMaths, MangaHigh, Reading Cloud and ShowMyHomework.

For access to any digital platforms, it is the responsibility of the Online Safety Co-ordinator to ensure all logins and passwords are secure and made available when required.

5. Educating parents about online safety

- The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website and social media channels. This policy will also be shared with parents.

- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headmaster and/or the DSL.
- Concerns or queries about this policy can be raised with the Headmaster and/or the DSL.

6. Cyber-bullying

6.1 Definition

- 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. (See also the Behaviour and Discipline policy.)

6.2 Preventing and addressing cyber-bullying

- 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.
- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSCHE) education, and other subjects where appropriate.
- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
- The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the Behaviour and Discipline policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- The DSL/DDSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or

- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the school's COVID-19 risk assessment.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendix 1, 2 and 3).

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.

8. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this 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
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix 3.

Work devices must be used solely for work activities.

If staff has any concerns over the security of their device, they must seek advice from the Online Safety Co-ordinator.

9. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our Behaviour and Discipline policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with Staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

10. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and DDSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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.

More information about safeguarding training is set out in our child protection and safeguarding policy.

11. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour and Discipline policy
- Complaints policy
- Taking, Storage and Using Images of Children policy
- Anti Bullying policy
- Social Media policy
- Computing policy
- Data protection policy and privacy notices

Appendix 1: Computer Usage and Internet Access Agreement for Parents

To parents of all pupils in Prep 3, 4, 5, 6, 7 and 8.

Dear Parents,

At Quainton Hall School we continue to increase the exposure that pupils have to computer systems as part of our teaching and their learning. The network that supports curriculum computing contains the Eyden Room suite, many PCs around the classrooms, and more tablets and laptops arriving each year. The children continue to use these more than ever before. The use of the computers and of the internet is almost entirely for school-related tasks, although there will be occasions when pupils will be using computers for recreational purposes.

Parents will be only too aware of the potential dangers involved in computer and internet use, and this document describes the rules for using these systems, along with the measures that the school has put in place to protect the pupils.

This usage agreement takes the form of a three-way agreement – Pupil, Parent and School, and we ask you to read this carefully, go through the contents with your child and sign it where marked on the final page. This is a new edition since parents were last asked to sign, so ALL are asked to sign this new agreement.

Each pupil from Prep 3 to Prep 8 is given their own username (and password) to access a secure folder on the network server, where they can store their own files. The username is not a secret, but the password is, and this should never be given to any other pupil. If a password is 'discovered' by another, it can of course be changed, but it is expected that such 'discoveries' will be very unusual!

Any pupil using the computer system to bully another will be punished in line with the School's anti-bullying policy. Members of staff are able, if necessary, to view **any file** stored in pupils' file storage areas on the server, and will do so if bullying is suspected.

Once logged in to the school network, the pupil's personal username and password can then also be used to gain access to our internet service. All material coming in to QHS by this means is filtered appropriately to the age of our pupils.

1. We expect all pupils (from Prep 3 upwards) to promise not to try to access sites which are not suitable. If a site which they know to be 'unsuitable' in some way is found by accident, they are expected to report it to Fr. Mike immediately. The current expectation is that pupils in Prep 3 to Prep 8 will get chances to "surf the net" without direct supervision in some lessons as well as some other open access times (lunchtime clubs, library time etc.). This access without direct supervision will only be granted to those who sign this agreement.
2. We ask parents to be aware of the nature of the Internet and that material that initially appears harmless may lead, via the web of links, to material which is unsuitable. Parents may well wish to install some sort of filtering on their home PC if their children are allowed unsupervised access there. Up-to-date advice is available to parents if needed. Locating the home computer in a shared family room is always the best option for ensuring ease of supervision while children are online.
3. We (the school) have taken, and will continue to take, all reasonable steps to ensure that pupils are not able to access inappropriate material on the internet. We will explain at school what is expected of them to enable them to surf without direct supervision. They will realise that, although most of the unsuitable material is being filtered out from their reach, it may still be possible to find inappropriate material on

apparently otherwise innocuous sites. If such material is found by accident the school will take steps to ensure that such material is not accessible again.

Pupils caught wilfully searching for, or attempting to access, material which is considered unsuitable will be punished. The operating system keeps a log of **all web addresses** visited and **all searches attempted**, and these are inspected on a regular basis.

"Unsuitable material" currently includes the following: racist material, offensive language, pornography, nudity, wrestling material (WWF and similar), chat rooms, online shopping etc. Pupil access to any of the social networking sites, such as **Facebook, Twitter, and Instagram** etc. is not allowed. This list will be extended in line with good practice and common sense **at any time** as the school thinks fit.

We have not set up e-mail addresses for all members of the school, and, for the time being at least, e-mail will only be composed, sent and received under direct staff supervision. Personal **web-mail use by pupils is not allowed**. Downloads of material from the Internet will only be allowed under direct staff supervision. Access to **YouTube** (and other similar video sharing sites) will only be allowed under staff direction. Some senior classes may be producing blogs or other documents which may be published online at some stage. Pupils will not be identifying themselves or their friends in this work, which will also be supervised by staff.

Pupils are taught **never** to give out personal details online (name, address, phone number etc.) and **never** to agree over the internet to meet anyone unless as a part of an approved school project and they are accompanied by a responsible adult.

These rules will be summarised and displayed in the Eyden Room Suite and other suitable locations for all to see, and as a constant reminder to the pupils of what is expected of them.

Pupils are bringing work in from home on USB memory sticks, which is of course useful and entirely sensible, but such devices are only to be used in school with staff permission.

Pupils who break the rules may be banned from future use of the facilities and additional punishment from the Headmaster will be severe. Parents will be involved in the matter immediately.

Many pupils are now bringing their own "smart" devices to school. These MUST be left at the School Office for safe keeping during the day. There will only be a very few special occasions where pupils are asked to bring such devices to lessons and, on these occasions, a request will be made via parents.

We ask that you and your child sign both copies of this document and return them both to me at school. I will then sign them both, return one copy to you and retain the other at school as a formal record of our agreement.

Thank you for your co-operation in helping to ensure that the use of our IT facilities can continue to thrive across the whole curriculum at school.

Fr. Mike Still

Online Safety Coordinator

Assistant Head (Administration)

Appendix 2: Computer Usage and Internet Access Agreement for Pupils

September 2020

Name of Pupil: .....

Network Username: (to be completed by Fr. Mike).....

This agreement is a formal statement of an undertaking made by the three parties involved, Parents, Pupils and the School.

PARENT or GUARDIAN - I undertake to support the school in educating the children on safe and intelligent use of a PC network and the internet.

Signed: ..... Date: .....

PUPIL - I promise not to use my access to a computer to bully anyone in any way. I promise not to use the internet to try to find material which I know to be unsuitable for me, and I promise to report immediately any site that I may find by accident that I think may not be right for me to see. I understand that I must never give out personal information (my own details or details of others) when using the internet.

Signed: ..... Date: .....

SCHOOL - We undertake to educate the children in how to use computers and the internet in a safe, constructive and productive manner and to take reasonable steps to ensure that unsuitable material is not available to pupils when they surf the internet on school premises.

Signed: ..... Date: .....

This agreement will last from the date of signature until the pupil leaves QHS, and a revision (with renewed agreement from Parent and Pupil) may be required at any reasonable time as circumstances change.

Appendix 3: Computer Usage and Internet Access Agreement for Staff

Agreement for Staff, Governors, Volunteers and Visitors of Quainton Hall School

When using Quainton Hall School's ICT systems and accessing the internet in school or outside school on a work device (if applicable), I will not:

- Access, or attempt to access any material which is inappropriate, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use my access in any way which could harm the school's reputation
- Access any social networking sites or chat rooms, unless it is in relation to my work or to fulfil the duties of my role
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first and in accordance with the Taking, Storage and Using Images of Children policy
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data either online or on the QHS servers that I am not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the QHS

I will contact the Online Safety Co-ordinator if I suspect my password may have been obtained by the third party.

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and Online Safety Co-ordinator know if a pupil informs me they have found any material, which might upset distress or harm them or others, and will do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Name:
Signed (staff member/ governor/volunteer/visitor):
Date: