Section 3.30 Online Safety Policy

Latest reviewed	February 2024
Review cycle	1 year

Issue Control		
Date to be reviewed	**Comment**	**Updated by**
February 2025		DSL

Introduction

It is the duty of Frensham Heights to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our students are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites and apps;
- Email and instant messaging;
- Blogs;
- Social Media & Networking sites;
- Music / video downloads;
- Gaming;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- AI tools;
- Online communities via games consoles; and
- Mobile internet devices such as smart phones and tablets.

This policy, supported by the The Use of Technology Policy (including Acceptable Use) Section 2.25 of staff handbook and available on Teams for Students in Year 7-13) is implemented to protect the interests and safety of the whole school community. The policy is also available

on the school website. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Child Protection and Safeguarding Policy
- The Use of Technology (including Acceptable Use Policy)
- Anti-Bullying Policy
- PSHE Policy
- Curriculum Policy
- Staff Behaviour & Code of Conduct
- Health & Safety Policy
- Behaviour Management Policy
- Data Protection Policy
- Use of Image Policy

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At Frensham Heights, we understand the responsibility to educate our students on online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving students in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas.

School Aims

Frensham Heights is a progressive co-educational day and boarding school educating and inspiring children from Nursery to Year 13. The School provides full-time education for students of compulsory school age (constructed in accordance with section 8 of the Education Act 1996). Frensham Heights wants every student to find future success and thus prepares them for their future and life beyond school. Providing the highest standard of academic education and high-quality pastoral care enables both boarders and day students to flourish within a happy school environment.

Frensham students are prepared for the ever-increasing challenges of the outside world. Through the progressive approach, they develop the confidence to understand who they are - physically, mentally and spiritually - and how they can make a difference now and in the future.

Frensham's values are:

1. **Originality of thought (Frensham embraces creativity):** We encourage everyone to foster their boldness and innovation, seeing opportunities locally and globally to discover and bring fresh thinking to our community
2. **Sprit of togetherness (Frensham nurtures community spirit):** Relationships are the foundation of our school and our success, built on genuine mutual respect, compassion and kindness. We embrace freedom with a firm understanding of our responsibility towards our community.
3. **Respect of individuality (Frensham celebrates authenticity):** This is a place where you can be the 'true you'; we pride ourselves on that. We support all to have the confidence to stand for something and be the person you truly want to be.
4. **Courage to try (Frensham fuels personal dedication):** We aspire to be the very best we can be, fully committing to our learning, proactively seeking improvement and working collaboratively for the benefit of the whole community.

These values are promoted through:

- Flexible high-quality teaching based on the individual needs and abilities of all students;
- Ensuring creativity of thought is utilised in all areas of the curriculum and wider school life;
- Guiding students to find their voice and their conscience through deep intellectual development;
- Emphasising emotional and mental wellbeing in all members of the Frensham community;
- Stimulating extracurricular, scholarship and enrichment opportunities.

These values are embedded in the curriculum and in particular in ICT and Horizons (PSHE) lessons where the delivery of Online safety principle happens. They also underpin the wider working of the school and its whole school approach to issues around Online safety.

Statutory Guidance and Requirements

Keeping Children Safe in Education (2023) the statutory guidance for schools and colleges endorses a 'whole school approach to online safety' and explains that this will include a clear policy on the use of mobile technology in the school. It recognised that all staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse other children online, this can take the form of abusive, harassing, misogynistic or misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content. This policy aims to meet that guidance.

The DfE's Boarding Schools National Minimum Standards requires schools to have and implement a policy that includes measures to combat cyber bullying and refers to how boarding students are supported in regards to their online behaviour. This policy meets these requirements.

The statutory guidance document '***Relationships Education, Relationships and Sex Education (RSE) and Health Education: statutory guidance for governing bodies, proprietors, head teachers, principals, senior leadership teams, teachers'*** clearly sets out curriculum content that secondary schools must deliver on what it describes as "Online Relationships", "Online and Media" and "Internet Safety and Harms" in order to keep students safe.

Frensham Heights follows this guidance in its delivery of online safety in ICT and Horizons (PSHE) lessons. The Horizons Department Handbook give details as to when this is planned to happen throughout the year. At times the planned timetable may be adapted due to specific local or national needs or the needs of our students, but Frensham Heights ensures that all required content is covered throughout the year. The Horizons Department Handbook can be found here. Appendix 1 outlines what is taught in ICT lessons. Together these meet all the requirements of this Statutory Guidance.

Scope of this Policy

This policy applies to all members of the school community, including staff, students, parents and visitors, who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents includes students' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the Acceptable Use Policy cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by students, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

Roles and responsibilities

1. The Governing Body

The governing body of the school is responsible for the approval of this policy and for reviewing its effectiveness. The governing body will review this policy at least annually.

2. Headteacher and the Senior Leadership Team

The Headteacher is responsible for the safety of the members of the school community and this includes responsibility for online safety. The Headteacher has delegated day-to-day responsibility to the DSL.

In particular, the role of the Headteacher and the Senior Leadership team is to ensure that:

a. staff, in particular the Deputy Head /DSL are adequately trained about online safety; and

b. staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the school.

3. Online safety coordinator

The DSL takes the role of the school's online safety coordinator. They are responsible to the Head for the day to day issues relating to online safety. The online safety coordinator, has responsibility for ensuring this policy is upheld by all members of the school community, and works with the Director of IT & Estates and all staff to achieve this. They will keep up to date on current online safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board.

4. Director of IT & Estates & Technical Support Staff

The school's Director of IT & Estates has a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, cloud based systems, its data and for training the school's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails and maintain content filters.

5. Staff

All staff are required to read the Use of Technology (including Acceptable Use Policy) Policy before accessing the school's systems as part of their induction.

As with all issues of safety at this school, staff are encouraged to have 'professional curiosity' when they see or hear something that looks unusual and to ensure that they create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis. Staff are trained in online safety regularly both in Staff Conference Safeguarding Updates delivered termly by the DSL and by completing annual online training courses in Online Safety.

ICT Teaching Staff and Horizons (PSHE) teaching staff are responsible for the delivery of online safety lessons as detailed in the annex below. These lessons are informed by the Statutory

Guidance on Relationships Education, Relationships and Sex Education (RSE) and Health Education and in the particular the 4 Cs of online safety educations: Content, Contact, Conduct, Commerce.

6. Students

Students are responsible for using the school IT systems in accordance with the Acceptable Use Policy, and for letting staff know if they see IT systems being misused. A copy of this document is available to them in Teams for their information at all times

Students are reminded that bringing in devices with preloaded movies/games/apps or material that is not age appropriate or suitable for our school environment will result in further conversations as needed; possible with sanctions being imposed. It is acknowledged that the school cannot control what students access via the 3/4/5G networks, but that it will always challenge concerning behaviour which it is made aware of. The Horizons schemes of work include multiple times when students are educated to support and educate them in this regard.

7. Parents and carers

Frensham Heights believes that it is essential for parents to be fully involved with promoting online safety both in and outside of school. We regularly consult and discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet The Online safety coordinator is supported by Jack Talman (Head of Horizons) who take the lead in providing resources to support parents. The school holds online safety coffee mornings and webinars for parents to help support them.

Parents are actively encouraged to share any concerns regarding online behaviours with school as soon as they are aware of them, so that in turn the school can follow up with conversations with other students and parents if needed.

8. Boarding Staff

We acknowledge that boarding students require a balance between accessing the online world for the sake on communications with home, entertainment and study, whilst also acknowledging its responsibility to provide a safe environment. Boarding staff will be particularly vigilant in both technology use and know that there is increased responsibility to share concerns with the pastoral leaders, the DSL and safeguarding team.

Use of school and personal devices, including mobile and smart technology

Staff

School devices assigned to a member of staff as part of their role have, by default, a password or device lock so that unauthorised people cannot access the content. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

Staff at Frensham are permitted to bring in personal devices for their own use and can access the schools Wi-Fi if needed.

The Staff Code of Conduct gives further information on social media and use of mobile phones in school

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored.

Staff must immediately report to Director of IT & Estates, or a member of SLT the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to Director of IT & Estates.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Frensham Heights into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive.

Any digital communication between staff and students or parents / carers must be professional in tone and content. Staff are advised not to contact a pupil or parent / carer using any personal email address. The school ensures that staff have access to their work

email address when offsite, for use as necessary on school business. Staff should not add school students or parents to personal social networks or social media accounts.

Students

Students in Year 7 and above at Frensham have collaborated with staff to produce a Code of Conduct regarding technology which is as follows:

During lessons: Tech should never be a distraction – it should be useful and purposeful.

- Mobile devices should be on silent in your bag as default (or on the desk face down if you don't have your bag)
- Mobile devices can be used if instructed or allowed by the teacher to:
    - Access O365
    - Research lesson content
    - Create media
    - Listening to music during extended tasks Volume should be so that you can still hear the teacher – and no one can hear your music. No faffing with playlists or sharing headphones etc
    - No social media or messaging

If you don't have a mobile device, then your teacher will ensure you have the resources you need to access at home (via Teams) or if essential for that lesson – by borrowing an ipad.

Outside of lessons: Our no phone zones:

- Library (music and work only)
- Theatre (unless requested by teacher)
- Dining hall (unless on your own)
- Toilets and changing rooms

Look where you are going and be aware of using your phone whilst moving around the campus, whether you are inside or outside – students wanted parents and staff to be aware of this as well! We will be providing mobile phone cabinets in areas of the school for you to lock, charge and store your mobile phones.

In the boarding houses:

HH – All tech should be handed in at night at sign in. Mobile phones are not to be used during prep - computers are available if needed.

MH – Students are allowed tech, however the wifi goes off at 10.30pm. This is because we feel working beyond this time is counterproductive. Students are given locked storage where phones are charged overnight.

RH – Students are allowed tech, however the wifi goes off at 11.30pm. This is because we feel working beyond this time is counterproductive. Students are given locked storage where phones can be charged overnight.

General:

- We will not take photos or video of each other without consent.
- We will T.H.I.N.K when posting, sharing and communicating with and about each other.

Consequences: If you misuse your mobile device, the teacher may take your phone from you and hand it to the Head of School or Assistant Head of School (or Deputy Head) for you to collect at a later time - normally at the next break or at the end of the day. If you break a school rule or the Acceptable Use Policy, then other sanctions may apply

All students are issued with their own personal school email addresses and Office 365 account for use on our network and by remote access. Access is via a personal login, which is password protected. Students should be aware that (email) communications through the school network and school email addresses are monitored.

There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work / research purposes, students should contact the Director of IT & Estates for assistance.

Students must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to a member of staff.

The school expects students to think carefully before they post any information online, or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Students must report any accidental access to materials of a violent or sexual nature directly to the a member of staff or Director of IT & Estates. Deliberate access to any inappropriate materials by a pupil is likely to lead to the incident being recorded on CPOMS and may be dealt with under the school's School Rules / Behaviour Management Policy. Students should be aware that all internet usage via the school's systems and its wifi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work / research purposes, students should contact the Director of IT & Estates for assistance.

Data Storage and Processing

The school takes its compliance with the Data Protection Act 1998 seriously. Please refer to the Data Protection Policy and the Use of Technology (including Acceptable Use Policy) for further details.

Staff and students are expected to save all data relating to their work to their Microsoft OneDrive account

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or students should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by school.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Director of IT & Estates.

Password security

Students and staff have individual school network logins [, email addresses] and storage folders on the server. Staff and students are regularly reminded of the need for password security.

All students and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which should be changed every [6] months;
- not write passwords down; and
- not share passwords with other students or staff.

Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.) without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other students in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy and the Acceptable Use Policy and the Staff Behaviour and Code of Conduct Policy concerning the sharing, distribution and publication of those images. If images are to be used, permission for use should be checked via the Annual Consent Form returns. Those images should be taken on school equipment where possible.

Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Students must not take, use, share, publish or distribute images of others without permission.

Written permission from parents or carers will be obtained before photographs of students / students are published on the school website via the Annual Single Consent form

Photographs published on the school website, or displayed elsewhere, that include students, will be selected carefully and will comply with good practice guidance on the use of such images. Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Misuse of Technology

Frensham Heights will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police and/or the LSCB. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from CEOP.

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with School Rules, Anti-Bullying or Child Protection and Safeguarding Policy.

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy. Where possible, we try and correlate online behaviours with 'in real life' behaviour

Wifi Filtering and Monitoring

The school follows the DfE Filtering and Monitoring Standards. The Director of IT & Estates and DSL have specific responsibility to manage filtering and monitoring systems and review these annually. The Smoothwall system blocks students from being able to access harmful and inappropriate content.

The school uses Smoothwall for its filtering system, and instant alerts (and daily summaries) are sent to the Director of IT & Estates and DSL, these are reviewed and actioned daily in line with Safeguarding and School Rules; with formal conversations noted on CPOMS. The highest level of alerts trigger text messages, teams messages instantly to key pastoral staff including the Director of IT & Estates and DSL and are acted on immediately.

All staff have been trained regarding the Wifi Filtering and Monitoring systems and are aware of how these work and how they can support students safety. This system is also included in the Safeguarding Induction given to all new members of staff. Staff monitor students online behaviour in lessons and every day interactions with students, particularly when using IT in the classroom.

The school recognises that, as stated in Keeping Children Safe in Education 2023, "many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content." Students are encouraged not to use 3G, 4G and 5G and this use is hampered by poor reception in the school's rural setting. Horizons and IT lessons offer multiple opportunities for staff to educate students about the risks and potential harms of this behaviour and so to encourage students not to engage in this. Any misuse of

technology in this way is responded to in line with the school's Safeguarding Policy as well as the School Ruled and Behaviour Policy.

Safeguarding & Prevent

The school has a separate Safeguarding Policy. Effective maintenance of Online safety provision across the school may bring about disclosures of safeguarding issues and staff are aware of the procedures for reporting their concerns through regular Safeguarding training. Staff are aware that the online world poses an equal risk and challenge to all areas of safeguarding

Online safety curriculum for SEN students

Similar to Horizons and all other lessons and activities in school, Frensham recognise that a one size fits all approach may not be appropriate to elements of online safety education and a more personalised or contextualised approach for more vulnerable children e.g. victims of abuse and SEND, may be needed. To address this the Head of Horizon liaises with Heads of School and the Deputy Head before teaching sensitive topics to ensure students who may be impacted are identified. Parents are communicated to in advance, and as needed, topics that are being covered are identified to students in advance.

Equal Opportunities Statement

The school is committed to the provision of Online safety lessons to all of its students. Frensham ensures that the Online safety curriculum is differentiated to meet the needs of all students so that they can access the curriculum, including those with mental health issues.

Monitoring and Evaluation

The implementation of this policy will be monitored and evaluated through the normal processes of Departmental Review that apply to all areas of the curriculum. This policy will be reviewed by the Governors in the first instance and reviewed by SLT annually thereafter.

Dissemination

The Online safety policy is shared with all staff and is available in the Staff Handbook from the Horizons (PSHE) coordinator, Designated Safeguarding Lead or Head of Junior School on request

Appendix1: ICT Lessons Overview

Topics covered in ICT Lessons at Frensham Heights School

Year 4

- Childnet Smart Crew resources – Safe, Meeting, Accepting, Reliable, Tell
- These lessons cover issues around staying safe on line, meeting others online and encourages telling of adults of anything felt inappropriate online.

Year 5

- Play, Like, Share – Resources from age '8-10' section of Ceop website www.ThinkUknow.co.uk
- These lesson cover issues around playing online games and interacting with online media.

Year 6

- Resources from Google Interland – reality, mindful sharing, kindness, security
- These lessons encourage an attitude of kindness online and teach about what can be trusted online and how to maintain security online.

Year 7

- Cyberbullying using Childnet resources; Use of IT policy & school rules; personal security, passwords, anti-virus; Copyright & fair use

Year 8

- Ethical use of computing; digital footprint & use of social media; Fake News

Year 9

- Copyright & permissions

Year 10 & 11

GCSE Options include:

- GCSE IT
- BTec ESports

Topics covered in Horizons (PSHE) lessons in the senior school include:

Year 7

- Online Abuse & Cyberbullying
- Communicating Online
- Online Stranger Danger

Year 8

- Online Choices & Sexting
- Online banter/bullying
- Digital Footprint
- Digital Literacy
- Digital Scams

Year 9

- Online Abuse
- Online Pornography Issues

Year 10

- Digital Footprint
- Online Reputation
- Online Relationships

Year 11

- Fraud & Cyber-crime
- Living Online & Mental Health

Year 12

- Impact of Pornography

- Living Online & Body Image
- Fake News

Year 13

- Online Reputation & Digital Footprint