

SAFEGUARDING 3: ONLINE SAFETY POLICY

Issued by:	First Deputy
Last review:	7 September 2022
Next review due:	1 September 2023
Most recent edit:	7 September 2022
Circulation:	Staff Governing Council Website Parents Students

The purpose of this policy is to provide guidance to employees of Benenden School (Kent) Limited and its subsidiaries (collectively 'Benenden' or 'the School').

The internet brings enormous benefits to the world of education and work, as well as being an integral part of people's social lives. At Benenden we believe in embracing the online world and educating pupils and staff to use technology responsibly and safely. The safe use of ICT is an issue of behaviour, education, infrastructure and monitoring; it is fundamental to safeguarding pupils and staff both in and out of School. The School takes all reasonable precautions to ensure that users access only age-appropriate material and to educate pupils about online dangers. However, experience shows that it is not possible to guard against every danger and so we take a proactive approach to minimising risks whilst also educating students so that they can respond appropriately to an unsafe situation.

Risks are considerably greater where devices are beyond the School's control (4G, 5G, social media platforms etc.) and so the education aspect of safeguarding in this area is particularly important. Getting students into safe habits when accessing the online world via our systems should enable them to make the right choices when using their own connections. A key part of the online safety support we provide is showing students how to apply controls and privacy settings to their own devices and accounts.

It is important to be aware that safeguarding concerns can happen solely offline or solely online, but that it is often the case that issues can happen concurrently both in the real world and online. Whenever considering any offline issue the staff involved should always explore whether there is also any online component.

Management of Online Safeguarding

Online safeguarding is the responsibility of the Online Safety Coordinator/Designated Safeguarding Lead (the Deputy Head Boarding & Pastoral Care) who is supported by an Online Safety Officer (the First Deputy), an Assistant Online Safety Officer (the Director of Digital Strategy and Innovation) the IT department and other members of the Safeguarding Team. Any online safeguarding issues (for staff or pupils) must be reported to the Online Safety Coordinator, who will work with the Kent Safeguarding Children Multi-Agency Partnership as needed.

The Online Safety Policy is formed of two sections and four annexes:

1. [Keeping Pupils Safe Online](#)
2. [Keeping Staff Safe Online](#)

Annexes

- A. [Pupil Acceptable and Safe Use of ICT Agreement](#)
- B. [Staff Acceptable and Safe Use of ICT Agreement](#)
- C. [Educational Annex](#)
- D. [Technical Information](#)

This policy is part of a wider set of Safeguarding Policies which are designed to protect and promote the welfare of children. The Safeguarding Policies, which can all be accessed [here](#), are:

1. Safeguarding and Child Protection
2. Anti-Bullying (including cyberbullying)
3. Child on child abuse
4. Online Safety and the Acceptable Use of ICT (this Policy)
5. Use of Reasonable Force
6. Anti-Radicalisation.

These Safeguarding Policies are supported by a number of other policies, which can be accessed [here](#):

1. Staff Code of Conduct
2. Data Protection
3. Whistleblowing
4. Recruitment
5. Disciplinary Procedure and Process

Staff should be aware that pupils and staff are vulnerable online as they can be subject to cyberbullying and online exploitation. In such cases, the Online Safety Policy must be read in conjunction with the Anti-Bullying, Peer on Peer abuse and Safeguarding and Child Protection Policies. The guidelines for responding to an incident or receiving a disclosure outlined in the Child Protection Policy are therefore most likely to be used when dealing with an online safeguarding incident. However, not all online incidents will be a safeguarding concern; some will be of a disciplinary nature, in which case the guidelines in this policy will apply.

The online world can also be a source of both sexual harassment and mis-information regarding healthy relationships. It is therefore important that the School's RSHE programme educates pupils around these online risks and gives guidance around reliable sources of advice around relationships and sex.

Safeguarding 3A: Keeping Pupils Safe Online

Staff have a dual responsibility: to use ICT safely and professionally themselves and to safeguard pupils' usage. This section deals with pupil use of ICT.

Reporting Online Safety Concerns

The School will manage Online Safety incidents in accordance with the relevant policy: Child Protection, Anti-Bullying, Anti-Radicalisation, Disciplinary Procedure, Peer on Peer or Pupil Behaviour as appropriate. Parents/carers will be informed of any significant incidents concerning pupils.

Procedure

1. If a pupil, member of staff, parent, guardian or anyone else raises an online concern, follow the guidance for Child Protection or Bullying concerns i.e.
 - a. Do not promise confidentiality. If a child asks you to keep a secret, explain that, in order for her to receive the help and support they need with a serious problem, it may well be necessary for you to speak to someone else. Emphasise that no one will be told who does not need to be told.
 - b. Listen carefully being non-judgemental, supportive and respectful. It is best to have another adult with you, who can be suggested by or agreed to by the child.
 - c. Ask to see evidence. If evidence is available, exercise caution in asking to view anything that may involve inappropriate images or videos.
 - d. Preserve the evidence, for example by collecting in the relevant device(s), but do not forward any illegal or inappropriate content, as you could fall foul of the law in sending inappropriate content yourself. Staff should not print out, screen shot or in any way reproduce any material that could be considered illegal or inappropriate.
 - e. Wait until the end of the disclosure and immediately write up a summary only recording the facts as the child presents them. Do not include any personal opinions from the note-taker.
 - f. Report your concern to a member of the Safeguarding Team, usually the Designated Safeguarding Lead but, in their absence, the Online Safety Officer and/or the Anti-Bullying Officer. Such concerns might include breaches of filtering, inappropriate searches suggesting pupils are a safeguarding concern, cyberbullying, illegal content, grooming etc.
2. The concern will be recorded on either the Safeguarding or Behaviour and Bullying log as appropriate. Advice will be given to the member of staff/pupil about the next steps.
3. Where there is cause for concern or fear that illegal activity has taken place or is taking place then the School will contact the Children's Safeguarding Team and/or Kent County E-Safety Officer and escalate the concern to the police. If the School is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County E-Safety Officer.

Cyberbullying (along with all other forms of bullying) of any member of the School community will not be tolerated. Full details are set out in the School's Anti-Bullying Policy.

The Child protection and Behaviour and Bullying logs are reviewed annually by the Safeguarding Committee to inform future planning of pupil, parent and staff education and how best to keep pupils safe.

Anyone who has concerns about any aspect of Online Safety should contact the Online Safety Coordinator.

Types of unsafe behaviour online

The DfE document 'Keeping Children Safe in Education' (September 2022) outlines four broad areas of risk relating to young people's activities online:

Content: being exposed to illegal, inappropriate or harmful material;
Contact: being subjected to harmful online interaction with other users; and
Conduct: personal online behaviour that increases the likelihood of, or causes, harm.
Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

The following table exemplifies some of the potential risks:

	AGGRESSIVE	SEXUAL	VALUES
CONTENT (Types of content pupils might see)	<ul style="list-style-type: none"> Violent/hate material 	<ul style="list-style-type: none"> Pornographic and unwelcome sexual content 	<ul style="list-style-type: none"> Biased, racist or misleading information or services Sexist, misogynist/misandrist material
CONTACT (Types of interaction which pupils may have online)	<ul style="list-style-type: none"> Bullying Harassment Stalking 	<ul style="list-style-type: none"> Meeting strangers Grooming Sexual harassment 	<ul style="list-style-type: none"> Self harm and unwelcome persuasions
CONDUCT (Types of behaviour a pupil might get involved in online)	<ul style="list-style-type: none"> Bullying Harassment 	<ul style="list-style-type: none"> Creating or uploading inappropriate material 	<ul style="list-style-type: none"> Misleading information or advice
COMMERCE (Types of content a pupil may be exposed to)	<ul style="list-style-type: none"> 	<ul style="list-style-type: none"> Accessing or creating paid-for sexual content 	<ul style="list-style-type: none"> Inappropriate material appearing in generic or targeted ads

The School attempts to minimise *Content* concerns through its filtering systems (see **3E: Technical Information**) and seeks to educate pupils about online safety, and resilience generally, to provide them with the tools they need to keep themselves safe from *Contact*, *Conduct* and Commerce issues.

The *Contact* and *Conduct* also represent potential routes to radicalisation and so it is important that staff do read this policy in conjunction with the [Anti-Radicalisation](#) policy. As the School is both a place of education and a home for pupils during term time, pupils have access to a wider range of sites, such as social networks, than might otherwise be the case in a day school. All pupils have laptops and mobile phones, and the majority have a tablet of some form or another and pupils are likely to be the first to have emerging technologies for which there is no specified guidance. Staff should exercise common sense in the use of such technologies and report any concerns to the Online Safety team.

In terms of pupil education, the School:

- Encourages pupils to work with us and tell us when they have concerns.
- Tries to maintain good channels of communication rather than 'over-blocking' sites, so that pupils let us know when they get into difficulties.
- Takes pupils through the Acceptable Use of ICT Policy every year in a House Order, asking pupils to sign the agreement online.



- Gives other reminders in Form Orders as well as in House Order about online behaviour.
- Has Whole School Prayers focusing on how to stay safe, as well as legal updates.
- Informs pupils when changes happen to keep them safe.
- Uses PSHEE/RSHE, PPD lessons, Computing lessons and the Pupil Induction Programme to promote safe behaviour online.
- Asks Big Sisters and Prefects to promote safe behaviour online and to work with pupils to ensure their privacy settings are up to date and appropriate.
- Keeps parents informed through lectures and newsletters.
- Reminds pupils annually about the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to anyone.
- Has a group of senior pupils, the 'Digital Leaders', who regularly visit House and talk to pupils about online safety issues.

Monitoring of online activity

The filtering software used by the School generates daily logs of any web searches that contain 'trigger' words that imply potentially unsafe online activity as well as logs of any attempts to access sites deemed unsafe. The logs of pupil activity are reviewed by the Online Safety Officer, though are also accessible by the Online Safety Coordinator/DSL, who will pass any issues on to the relevant HM to follow up on. The logs of staff activity are reviewed by the Online Safety Officer, though are also accessible by the Director of Finance and Operations, who will follow up any issues directly with members of staff. A log of these issues is kept and is reviewed once a year by the Safeguarding committee. The Online Safety Officer maintains close contact with the Technical IT Services Delivery Manager to ensure that the list of trigger words is kept up to date with any emerging issues.

Pupil Use of Mobile device

Please use the following link for detail on when pupils in IV to UV may have their devices, as well as further guidance on their use:

[ACCEPTABLE USE OF MOBILE PHONES AND HANDHELD DEVICES](#)

In some instances, such as Enquiry Weeks and trips, younger pupils may be requested to bring their mobiles with them in order to make use of facilities such as the camera or as an additional means of safeguarding pupils when off-site.

Mobile phones are great for keeping in touch but they also provide an opportunity for people to send inappropriate messages to one another very easily and without thinking of the consequences. Staff may confiscate a phone or device if they believe it is being used to contravene the School's Behaviour or Anti-Bullying Policies. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence, the phone will be handed over to the police for further investigation.

Safeguarding 3B: Keeping Staff Safe Online

All staff sign an Acceptable Use of ICT (AUP) agreement (see Appendix 1) which outlines the steps they will take to behave in a safe and professional manner online. Staff should be aware that their online conduct out of School could have an impact on their role and reputation within School. Civil, legal or disciplinary action could be taken if they are found to bring the profession or the School into disrepute, or if something is felt to have undermined confidence in their professional abilities. Online behaviour must always be compatible with UK law.

Staff are required to maintain the professional standards demanded of adults working in a School who, by virtue of their employment are in a position of power, influence and trust. All staff are required to be familiar with the Staff Code of Conduct policy, which outlines appropriate behaviour in both the online and offline world. They should protect the reputation of the School and of themselves in the real and the virtual world.

If a member of staff discovers an online safety issue concerning pupils or staff, whether deliberate or not, the member of staff should immediately contact the Online Safety Coordinator or the IT Services Manager, as appropriate. A member of staff failing to report an issue would be in breach of the AUP which could lead to disciplinary action.

Management of Social Networking, Social Media and Personal Publishing

1. All members of the School community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory and they are reminded that what is posted online may be viewed by a large audience and may remain there forever.
2. Staff may have private social media accounts but may not 'be friends' with, 'follow' or in any other way engage with current pupils using private social media accounts, as this would cross a professional boundary. Staff may be 'friends' with Benenden Seniors, but only when the Seniors are at least 21 years old, and should be aware that Seniors may be linked to current pupils. Staff may have other roles outside of School in which they may need to use social media platforms, non-School email accounts etc to contact current pupils or recent Seniors under 21 years old. In such cases, the staff member must inform the First Deputy of this.
3. Staff members must ensure their security settings are private. Private social media accounts need to be used in a manner that does not bring the member of staff or the School into disrepute or affect their professional status.
4. Staff must take particular care if they choose to make reference to the School in any private posts, that they do not make damaging statements which could adversely affect the reputation of the School.
5. Staff have a duty to behave in a professional manner, even in their private posts, as any information posted online could compromise their ability to discharge their duty as a member of School staff working with young people. Teachers in particular should be aware that the DfE's *Teachers' Standards* (2012) state that 'a teacher is expected to demonstrate consistently high standards of personal and professional conduct'.
6. A department may establish a link with Seniors by setting up a separate departmental Facebook site or other social media account and this should have privacy settings which only allow access to a specific group of seniors. These sites should be registered with the Online Safety Coordinator.
7. If a member of staff wishes to set up an official blog or wiki which is linked or can be tracked back to the School, permission should be sought from the Online Safety Coordinator. Such a site should be password protected and run from the School website.
8. Staff are able to set up work-specific social media accounts, using their School email address, in order to be able to teach pupils the safe and responsible use of Facebook or other social media or for other educational reasons such as revision for exams. These sites should be registered with the Online Safety Coordinator. Profiles of pupils and the members of staff must be different from and unlinked to their personal profiles.

Management of mobile phones and personal devices

Staff should not use their own personal phones or devices for contacting pupils and their families. School mobile phones are available for trips. If this is likely to be an issue for a particular event then speak to the Assistant Head: Head of Co-curricular for advice.

Where staff wish to take photographs of pupils during School activities and trips, all photographs must be taken on School devices. Houses should have a House device to use and anyone running a trip can organise for a device via the Domestic Bursar's Office. If this is likely to prove difficult then speak to the Online Safety Officer or Assistant Head: Head of Co-curricular for advice.

The agreement for managing personal devices is outlined in the AUP.

Management of Email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of School, email should not be considered private.

The School gives many members of staff their own email account to use for all School business. It is the responsibility of each account holder to keep the password secure. Staff will be prompted at regular intervals to change their password in order to maintain a high level of security, and should avoid using passwords that they use for any personal accounts. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. Staff must not contact pupils or parents to conduct any School business using personal email addresses and should avoid using School email addresses for personal business.

All email users are expected to use appropriate language in email communication and not to write anything defamatory, unpleasant or untrue about another person. Staff must inform the Online Safety Coordinator if they receive an offensive email.

It is quite common these days to receive emails from unknown sources which may contain links, or attachments. Great care should be taken with these emails and simple rules should be followed to maintain the security of any system.

Unexpected attachments, even from people you know, should not be opened as they may contain malicious software.

Emails containing links may be a 'phishing' email, clicking on the link may well take you to a site where you are asked for your email and password. Look out for these kinds of emails, clues that they are fraudulent are often found in the quality of the written English, or hover (not clicking) over the link to see the actual address you would be directed to. If you suspect an email is a phishing attack simply delete it. The School will periodically run a mock phishing attack and the results will be reviewed.

Safeguarding 3 Annex A: Pupil Acceptable and Safe Use of ICT Agreement

This document is explained to pupils annually as part of a House Order and pupils will then be required to 'sign' an online form agreeing to abide by these rules.

It is important that you realise that the power of the online world brings certain responsibilities to yourself and towards others. You must not misuse the network to hurt others or put yourself in danger. Breaching these requirements will result in appropriate sanctions in order to encourage safer behaviour in future.

Using the Network

- I will not attempt to log on as someone else or to access folders and files I do not have permission to use. I will not share my login details with others.
- I will not install software, including screen savers, on the School machines.

Communication (email etc.)

- I will not send offensive messages or pictures, use obscene language or use email to bully fellow students, harass, insult or otherwise annoy others.
- I will only access or use my email in lessons if I have specifically been asked to by my teacher.

I should not tolerate receiving offensive messages and can report any problems to my tutor, my HM, the Online Safety Officer, a member of the Safeguarding team or anyone else with whom I feel comfortable.

The Internet

- I will not try to enter websites that obviously contain forbidden* material (see definition below).
- I will not attempt to by-pass the School's internet filtering systems.
- I will not download files containing forbidden material unless my teacher specifically arranges for access to the material as part of my studies.
- I will not pass off material downloaded from the internet as my own as this is plagiarism.
- I will only access the internet in lessons if I have specifically been asked to by my teacher.
- I will not type in bad or sexually inappropriate language.

I understand that all web access is logged automatically and inspected daily and that inappropriate use of the internet will result in sanctions, usually beginning with a Blue Slip on the first occasion

Social media platforms (Twitter, Instagram, Snapchat, Facebook, TikTok, Youtube etc.)

- I am aware that under 13's should not have access to these platforms.
- I will ensure that notification alerts are turned off during lessons and all events.
- I will not post offensive comments on any social network or website as this is illegal.
- I will only upload content concerning the School, or using its name, after gaining permission from the Deputy Head Boarding and Pastoral Care.
- I will only access or use social networks in lessons if I have specifically been asked to by my teacher.
- When posting videos or photographs (referred to as images from here on) I will follow these guidelines:
 - Images are to ONLY be taken in public areas and not where a student might expect privacy (eg Showers, changing rooms etc).
 - Images should be of students who are fully dressed.
 - All people in an image need to give consent for an image to be shared or stored, even if they are accidentally photographed or filmed.

- I should be careful when posting images that the School is not identified or that names of fellow students are mentioned.
- I will inform my HM if I am posting regularly on a public channel and am aware that this information will be logged.

Entrepreneurship and Mentoring

The School encourages students to be entrepreneurial and offers a variety of opportunities to students to run their own business or work with professional mentors during business or enterprise projects or competitions. This might involve online mentoring, possibly through Benenden Connects. For Sixth Form students, you may undertake some virtual work experience. The School will help you remain safe whilst doing this.

- If you do wish to set up a business with an online presence we expect you to inform the Online Safeguarding team via your HM.
- The School name, logo etc should only be used with permission.
- Images used to promote products should follow the guidelines for images set out above.
- Appropriate safeguarding checks will have been undertaken by the school for any work experience or mentoring

Mobile and Smart Devices

I understand that all of the above rules apply equally to the use of mobile devices including smart phones, tablets, hand-held gaming devices and laptops.

Taking images or videos in House and around School

I am aware that taking images (which includes videos as well as still pictures) needs to be carefully managed and that in terms of taking images:

- Changing times and areas are off limits.
- Showers/toilets are off limits.
- Images must not be taken of pupils in towels, swimsuits or inappropriate nightwear.
- Images must not be taken of pupils who are naked.
- I should get permission from others to take images of them and make clear what I intend to do with the image.
- I need to be aware that people might be accidentally caught in the background of a shot – if this happens I will delete the picture/video unless those caught give permission to use the image

I should not have to tolerate others taking images of me without my permission. I have the right to ask that images of me are deleted and not posted online.

Saved work

I will not save anything to School provided storage (network or cloud) that breaks the above rules.

I understand that to protect all students, particularly when investigating misuse of ICT and certainly where the personal security of students is involved, the School can have access to student files and emails.

My online behaviour outside of School may have consequences in school, particularly where it may involve other Benenden pupils or use of the School name.

***Forbidden and Inappropriate Material**

Examples of forbidden or inappropriate material include: pornographic material, material promoting the use of drugs, harmful behaviours, politically extremist and violent material, racist material and the



use of bad, sexually inappropriate or explicit language. Generally, it is material that you would not wish parents or teachers to see. The School's filtering systems protect access to forbidden material; however, you must be on guard in case a site is allowed through the filter by mistake. Such sites should be reported immediately to a member of staff.

Consequences

I am aware that if I break this agreement, sanctions will apply. Blue Slips and detentions will be given for more minor offences, but temporary exclusion or permanent exclusion could result from very serious offences such as repeated or extremely serious cyberbullying.

I will always check with a member of staff if I am unsure whether certain uses of ICT are appropriate or not.

Name of Student

House

I have read the *Acceptable ICT Use* notes and agree to abide by the points mentioned. I will use the facilities in a responsible way and observe all the restrictions.

Student signature

Date



Safeguarding 3 Annex B: Staff Acceptable and Safe Use of ICT Agreement

As part of a professional organisation with responsibility for children's safeguarding, it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the School's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information & Communication Technology and the School systems, they are asked to read and sign this Acceptable Use Policy. This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the School ethos, other appropriate policies and the law.

Further guidance on other aspects of appropriate behaviour is available in the [Staff Code of Conduct](#).

Definition

I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites.

If I have any questions or concerns I will take these to the Online Safety Coordinator, Online Safety Officer or Head of IT Support as appropriate.

Professional and Legal Obligations

1. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation. I will therefore use School-owned information systems appropriately and within the law.
2. I will respect copyright and intellectual property rights.
3. My use of ICT and information systems will always be compatible with my professional role, whether using School or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will be in accordance with the School ethos and the law. It will not contain any inappropriate language nor any defamatory or libellous comments; it will not contravene the School's [Equality Policy](#), e.g. in respect of gender, race, age, sexual orientation, religion or beliefs, or any other protected characteristic.
4. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, or the School, into disrepute.
5. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Online Safety Coordinator or the Technical IT Services Delivery Manager as soon as possible.
6. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead/Online Safety Coordinator as soon as possible. In their absence I will report any concerns to the Online Safety Officer or another member of the Safeguarding team.
7. I will promote safe internet use with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

**Security**

1. I will respect system security and I will not disclose any password or security information.
2. To prevent unauthorised access to systems or personal data, I will not leave any device unattended without first logging out or locking my login as appropriate.
3. When I am away from School, including working on one of my own devices, I will ensure that no one gains access to the School network, systems or personal data via my username.
4. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the Technical IT Services Delivery Manager as soon as possible. and any personal devices I connect to the school network will have up-to-date anti-virus software working.
5. I will not attempt to bypass any filtering and/or security systems put in place by the School. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any School-related documents or files, then I will report this to the IT Services Dept as soon as possible.
6. In the event of my not being in school, e.g. through illness, I understand that the School may access my folders and email to recover important documents. Where possible I will be asked to give permission for this but will always be informed if this is to happen.

Data and Data Protection

1. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998 (DPA) and the European General Data Protection Regulations (GDPR) and images or videos of pupils will be used in line with the School's [Data Protection Policy](#) and will always take into account parental consent.
2. I will not keep professional documents which contain School-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones, memory sticks) or on a Cloud-storage system, unless they are secured and encrypted. This also applies to file-sharing platforms such as Dropbox and WeTransfer, please seek advice from the IT Support department before using any such platforms. I will protect the devices in my care from unapproved access or theft.
3. Any photographs taken on personal devices will be downloaded onto the School network or to a School device within 24 hours and deleted from the personal device. However, where possible, I will always use School equipment to take photographic images.
4. I will use School telephones/mobiles rather than my own devices to contact pupils and parents. Where this is not possible I will block my number or ask that the recipient delete it from their device.
5. I will not store any personal data on the School computer system without the written permission of IT Services.

Where it believes unauthorised and/or inappropriate use of the information systems or unacceptable or inappropriate behaviour may be taking place, the school will invoke its disciplinary procedure. If the school suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with the School's Online Safety Policy and Staff Acceptable Use of ICT Policy

Signed:

Print Name

Date

Safeguarding 3 Annex C: Classroom use of ICT

Pupil Use of Laptops and Tablets

The use of laptops and tablets is encouraged in the classroom as an aid to education. There should be a clear reason for the use of the device and pupils should be made aware of what they are and are not allowed to do. Staff should ensure they walk around the classroom when computers are being used so they can see what is being accessed on the screens. This is particularly important during prep times where pupils may be accessing a range of sites or programmes; staff should be confident in engaging with pupils to ask why they are accessing a particular resource.

The use of technology in classrooms presents some potential challenges in terms of behaviour management but it is important to focus on the behaviour rather than on the technology. Setting clear rules and expectations, as you would with any other aspect of pupils' work, should pre-empt most potential problems. Although pupils do have Computing lessons in IV-LV it is worth checking that pupils know how to use a particular piece of software (even those you may consider to be basic office packages) in advance of a lesson as this will also help to head off any issues.

If you plan to set preps that require the use of particular software, it is advisable to check with pupils that they have it available on their own devices or to contact the IT Support department (helpdesk@) to see whether it is available on the networked PCs.

There will be some pupils with Specific Learning Difficulties for whom the use of a laptop has been agreed as a way of supporting their learning. Staff should be aware of who these pupils are (via the Academic Support register) and allow them to use their laptops for any activity where this is practical. This extends to class tests where there is likely to be a large amount of writing.

It may be necessary at times for teachers or senior pupils to request that access to specified websites be granted in order to carry out School work. *Teachers* should make requests to the IT Support department in good time for this to be resolved before their lesson – the IT Support department will pass requests on to the Online Safety Coordinator if there is any concern about the websites to be accessed. *Pupils* must seek the permission of the Online Safety Coordinator first, who will then contact IT Support if the request is approved.

Safeguarding 3 Annex D: Technical information

Monitoring Usage of the School Network, Information Systems and Wi-Fi

Pupils', staff and visitors' use of the School's network, information systems, the internet and email is monitored to protect the interests of individuals and the reputation of the School. Web access is filtered by *Lightspeed* to prohibit access to forbidden material and to provide age-appropriate access to other sites. Web activity is logged automatically and daily checks are made of alerts to searches or web site visits containing, amongst other things, terrorist, sexual abusive and self-abuse language. Records of suspicious searches are reviewed by the Online Safety Coordinator and Online Safety Officer, who will follow up as appropriate with the pupil or member of staff who executed the search. In the case of pupils, alerts may be passed on a member of the pupil's House team to discuss with them but any cases will only be considered 'closed' once reviewed by the DSL or a DDSL.

The services provided by Lightspeed conform to the standards set out by the UK Safer Internet Centre for 'Appropriate Monitoring for Schools' and 'Appropriate Filtering for Schools'

All pupil and staff devices must be registered on the network before access to Wi-Fi is granted, this ensures that their online access can be appropriately monitored and filtered.

In exceptional circumstances, the School will access files and email in order to protect the interests of staff and pupils as well as the School's reputation. This will not be done routinely but may take place when investigating breaches of this policy. Such investigations will only be conducted with the agreement of a member of SMT.

Password Management

Staff and students are issued with a temporary password on arrival and advised to change as soon as possible. Passwords have to be a minimum of 6 characters long (though 8 or more is preferable) and they must contain a combination of at least any 3 of the following:

Upper case characters (A-Z)

Lower case characters (a-z)

Numbers (0-9)

Special characters (eg. !, @, #, &)

Staff and students are required to change their password every 120 days.