Halliford School
SHEPPERTON

Digital Safety Policy

March 2024

Approved by the Governing Body March 2024
To be reviewed March 2025

Contents

Mission Statement

Halliford is a school based on strong family values where we know and respect every student as an individual. We encourage and support Hallifordians to flourish and become the best version of themselves that they can possibly be.

We aim for excellence by being academically ambitious but at the same time academically sensitive.

We inspire Hallifordians within a community that is founded on high quality teaching and learning, outstanding pastoral care and first class sporting, cultural and co-curricular opportunities.

Aims of this policy

1. To ensure the safeguarding of all students within Halliford School by detailing appropriate and acceptable use of all online and digital technologies.
2. To outline the roles and responsibilities of all students, staff and parents.
3. To ensure all students, staff and parents are clear about procedures for misuse of any online technologies.
4. To develop links with parents and the wider community to ensure continued awareness of online technologies.

Introduction

Digital Safety encompasses any use of a digital device and/or wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to have the necessary knowledge and behaviours that can help them navigate the online world safely.

The school's Digital Safety policy will operate in conjunction with other policies. This includes the BYOD Policy (Appendix 4) and Microsoft Go Protocol (Appendix 7), and also those for Anti-Bullying, Teaching and Learning, Data Protection, PSHE, Safeguarding and Child Protection and the Safe Students Safe Staff Policy.

Digital Safety is a priority at Halliford School. While we actively embrace all of the benefits of the internet, we are equally vigorous in embedding safe working practices and teaching amongst the whole school community. We are committed to ensuring that we balance the life-giving and creative elements of this learning with an approach which brings best practice in enabling responsible behaviour for learning and wellbeing.

This Digital Safety Policy sets out the roles, responsibilities and procedures for the acceptable, safe, and responsible use of all digital and communication technologies, including the use of school based devices, the internet, email, instant messaging and other social networking technologies and mobile phones and games, to safeguard adults and students. It details how Halliford School will provide support and guidance to parents and the wider community (where appropriate) for the safe and responsible use of these technologies. It also explains procedures for any unacceptable use or misuse of these technologies by adults or students.

The use of the internet as a tool to develop teaching, learning and administration has become an integral part of school and home life. There are always going to be risks with using any form of

communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst students use these technologies. These risks include:

- Being vulnerable to inappropriate contact from strangers;
- Cyber-bullying;
- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or mobile devices;
- Issues with spam and other inappropriate email;
- Online content which is abusive, offensive, or pornographic;
- The use of social media to encourage extremism; and
- Viruses.

It is also important that staff are clear about the procedures, for example only contacting students about homework via a school email address or Microsoft Teams, not via personal emails.

Whilst we endeavour to safeguard and mitigate against all risks, we will never be able to completely eliminate them all. Any incidents that may come to our notice will be dealt with quickly and according to Halliford School's policies to ensure the school continues to protect students.

It is the duty of Halliford School to ensure that students, teachers, administrative staff and visitors are protected from potential harm whilst they are on school premises.

The involvement of students and parents is also vital to the successful use of digital technologies. This policy thus also aims to inform how parents and students are part of the procedures and how students are educated to be safe and responsible users so that they can make good judgments about information they see, find and use.

The Role of Technology in our students' lives

Technology plays an enormously important part in the lives of all young people. Games consoles, together with WiFi-enabled mobile phones provide unlimited access to the internet, messaging, to blogging, to social media websites (like Twitter), to Skype and FaceTime (video calls, via web cameras built into computers), to wikis (collaborative web pages), chat rooms and other social networking sites, and video sharing sites (such as YouTube).

This communications revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of the school's role to teach students how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, stalking and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment from their online reputation and subsequent digital footprint.

"Children and young people need to be empowered to keep themselves safe - this isn't just about a top-down approach. Children will be children - pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends; but we also teach children how to swim."

Dr Tanya Byron "Safer Children in a digital world: the report of the Byron Review"

The Four Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and seminudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Good Habits

Digital safety depends on effective practice at a number of levels:

- Establishing a listening and telling culture where students know the school will act, and that when they report they will be kept informed about what is happening.
- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies. This includes the use of devices in lessons across the school.
- Sound implementation of Digital Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure Internet access including the effective management of content filtering.
- Regular and effective training for staff and student appropriate workshops.
- Regular review of trends, reporting and what we are learning from student voice.
- Daily shutdown and full restart to ensure all updates are deployed on devices.

Students

Our students:

- Are involved in the review of our Digital Safety Agreement through discussion in lessons and our student e-safety forums, in an age appropriate way;
- Are responsible for following the Student Acceptable User Policy (AUP) whilst within school as agreed each academic year or whenever a new student starts at Halliford School for the first time, and required to sign that they have read and understood the rules;
- Are taught to use the internet in a safe and responsible manner through, for example, Computing, PSHE /RSE lessons and assemblies as well as observing Safer Internet Day (Appendix 9);
- Are provided with workshops on E-Safety from external industry experts at an age appropriate level on a regular basis through the PSHE / RSE curriculum;
- Are taught to immediately tell an adult about any inappropriate materials or contact from someone they do not know;
- Are made aware of the potential use of online digital technologies to expose young people to inappropriate contact from strangers and to extremist ideas and know what to do if they encounter such issues;
- Are taught and encouraged to consider the implications for misusing the internet and, for example, posting inappropriate materials to websites;
- Are taught that the downloading of materials, for example music files and photographs, needs to be appropriate and 'fit for purpose', based on research for school work, and be copyright free;
- Are taught to understand what is meant by digital safety through age appropriate delivery in accordance with Education for a Connected World Framework.
- Are taught that sending malicious or hurtful messages outside of school can become a matter whereby Halliford School may set sanctions or involve outside agencies such as the police;
- Are taught not to put themselves at risk online or through mobile phone use and taught what to do if they are concerned they have put themselves at risk;
- Are given explicit guidelines and procedures for using mobile phones and other personal devices in school and are expected to abide by this Digital Safety Policy; and the Student Acceptable User Policy (AUP)
- Are provided with a copy of the Student Digital Guide which includes a wealth of information of E-Safety and Responsible Digital Use.

Inappropriate use by students

Should a student be found to deliberately misuse digital or online facilities whilst at school, appropriate sanctions will be applied. If a student accidentally accesses inappropriate materials, the student is expected to report this to an appropriate member of staff immediately and take action to minimise the screen or close the window.

Deliberate abuse or damage of school equipment will result in parents being charged for the replacement costs of the equipment. Should a student use the internet whilst not on School premises in such a way as to cause hurt or harm to a member of School community, Halliford School will act quickly and in accordance with our Behaviour Policy.

Please refer to Annex 1 for further guidance.

Staff

It is the responsibility of all adults within Halliford School to:

- Adhere to the Safe Students Safe Staff Policy and the Staff Acceptable Use Policy (AUP);
- Complete regular GDPR training & E-Safety training (SWGfL)
- Implement the Student Acceptable Use Policy (AUP) (see Appendix 2);
- Be up to date with digital knowledge appropriate for different age groups;
- Be vigilant when using technology as part of lessons;
- Model safe and responsible use of technology;
- Provide reminders and guidance to students on Digital Safety;
- Ensure that students are protected and supported in their use of online technologies, and that they know how to use them in a safe and responsible manner;
- Understand that any student can be vulnerable online, and this can fluctuate depending on their age, developmental stage and personal circumstance. However there are some, such as looked after children or those with SENs, who may be more susceptible.
- Not leave a computer or other device unattended whilst they are logged on;
- Lock away or safely secure all portable ICT equipment when not in use;
- Not connect with any student under the age of nineteen on any social networking site, or via personal mobile phones and follow Halliford School's Social Guidelines. See Appendix 5 & 5 for further detail;
- Protect confidentiality and not disclose information from the network, or pass on security passwords;
- Make sure that any information subject to Data Protection is not stored on unencrypted portable media or transported in an insecure form;
- Use their discretion when communicating electronically about work-related issues and not bring Halliford School's reputation into disrepute;
- Follow Halliford School's 'dos' and 'don'ts' in our Email Best Practice Guide – see Appendix 6;
- Not make or take personal calls or engage in personal texting when they are on duty;
- Report any concerns about a student related to safeguarding and Digital Safety to the Designated Safeguarding Lead;
- Report accidental access to inappropriate materials to the Designated Safeguarding Lead so that inappropriate sites are added to the restricted list; and
- Only use school owned devices and memory cards to take photographs or videos.

Inappropriate use by staff

If a member of staff is believed to have misused the internet or network in an abusive or illegal manner from school, a report must be made to the Headmaster immediately. Safeguarding procedures must be followed to deal with any serious misuse, a report filed, and all appropriate authorities contacted as necessary.

Please refer to Appendix 1 for further guidance.

Parents and visitors

All parents have access to a copy of this Digital Safety Policy on our website. Parents are asked to explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted. Parents are also provided with the student Digital Guide and workshops from visiting speakers on E-Safety.

As part of the approach to developing digital safety awareness with students, the School may offer parents the opportunity to find out more about how they can support Halliford School to keep their child safe whilst using online technologies beyond school; this may be by offering parent education sessions or by providing advice and links to useful websites. Halliford School wishes to promote a positive attitude to using the internet and therefore asks parents to support their child's learning and understanding of how to use online technologies safely and responsibly.

Parents should be aware that Halliford School cannot take responsibility for a student's misuse or abuse of IT equipment when they are not on the School premises. This includes social networking with other students, and the possibility of students accessing inappropriate content. However, should parents or guardians become aware of an issue, we strongly encourage prompt communication with the School so we can offer advice and support. Halliford School has a duty to report serious concerns to local authority safeguarding teams or to the police, in line with statutory requirements.

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

- What are the issues? – What are the issues? - UK Safer Internet Centre
- Hot topics – Help & advice | Childnet
- Parent resource sheet – Parents and Carers resource sheet | Childnet

While the DSL/DDSLs may check emails intermittently at weekends or during the holidays and pick up monitoring alerts, it is the responsibility of parents to keep their child safe outside of normal school hours. If the alert is deemed 'high risk', parents will be alerted as soon as possible.

Wi-Fi access

Students, parents and visitors to Halliford School are expected to abide by this policy. Should visitors wish to access the internet via Halliford School's Wi-Fi, they will be issued with a temporary password. Access is only permitted once they have agreed to Halliford School's terms and conditions.

Video and photography at school events

Parents are asked to be considerate when taking videos or photographs at school events and are requested not to publish material of other children in any public forum without the permission of the relevant family.

It is illegal to sell or distribute recordings from events without permission. Any parent who does not wish for their child to be videoed or photographed at school events by other attendees must notify Halliford School in advance and in writing.

Bring Your Own Device (BYOD)

Clear procedures are in place for managing BYOD, including the requirement for signed agreements from parents and students. See the discreet BYOD Policy for staff and students, alongside Appendix 4

BYOD for students and staff is mac address controlled to enable effective monitoring of access to the school systems.

Halliford School's responsibilities

Halliford School takes its responsibilities in relation to the acceptable use of technology by students and adults seriously and understands the importance of monitoring, evaluating and reviewing its procedures regularly.

Filtering and safeguarding measures

Halliford School's internet has a robust filtering system (SENSO) which is set at an age appropriate level such that inappropriate content is filtered. The system logs all attempts to access the internet, including all attempts to access inappropriate content. This runs through both the network and BYOD access to wifi, along with other school controlled portals. All access is controlled by alerts, which are immediately brought to the attention of the Deputy Head Pastoral and in serious cases to the Headmaster. Regular audits take place of the alerts and patterns and trends are addressed if evident.

Filtering and safeguarding for school owned equipment is via the Senso Client. This has proven to be an extremely effective tool. Also all upstream DNS is via Cisco umbrella with filtering enabled as a secondary check.

ESET ENDPOINT Anti-virus, anti-spyware, anti-phishing software is installed on school owned devices. Emails are part of the schools Microsoft 365 tenant which deals with, among other things, junk mail and SPAM. Suspicious email activity has an auto account suspension facility and risky sign-ins are highlighted to the Network team for further investigation.

On and off premise files are profile and user secured to ensure information about our students cannot be accessed by unauthorised users.

The wireless network has a cloud based controller which reports on issues and has automatic firmware updates and security updates.

Email use

Halliford School provides school email addresses for students (Year 7 – Upper Sixth) to promote safe and efficient communication.

All students and staff are expected to use email professionally and responsibly. All staff – teaching and administration have mandatory 2fa enforced. See Appendix 7 for further details.

Use of images and videos

Halliford School abides by the Data Protection Act 1998 and understands that an image or video is considered personal data. It seeks written consent from parents to publish images or videos for external publicity purposes, such as the website, and for internal purposes, such as a yearbook or on a parent portal. Parents and guardians may withdraw their permission at any time by informing the administration team in writing.

Staff are not permitted to use their own devices or memory cards to record videos or photographs of students, and when storing images within Halliford School's network are requested to only use the student's first name.

The curriculum and tools for learning

Halliford School teaches our students how to use the internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding, and communicating effectively in order to further learning, through Computing and/or PSHE / RSE lessons. The following concepts, skills and competencies are taught through Halliford School in an age appropriate manner:

- Digital citizenship;
- Future work skills;
- Internet literacy;
- Making good judgments about websites and emails received;
- Knowledge of risks such as viruses, and opening mail from a stranger;
- Access to resources that outline how to be safe and responsible when using any online technologies;
- Knowledge of copyright and plagiarism issues;
- File-sharing and downloading illegal content;
- Uploading information – knowing what is safe to upload, and not to upload personal information; and
- Where to go for advice and how to report abuse.

These skills are taught explicitly within the Computing curriculum but are likely to be covered in other subjects; students are taught skills to explore how online technologies can be used effectively, in a safe and responsible manner. Further details about the content of the curriculum related to ICT can be found in the Computer Science and PSHE curriculum documentation.

Monitoring

It is the responsibility of Halliford School to ensure appropriate systems and technologies are in place to monitor and maintain the safeguarding and security of everyone using the School network. Halliford School will monitor the use of online technologies and the use of the internet by students and staff. The Designated Safeguarding Lead, Computer Science teachers and the SMT will conduct regular audits with students to assess their knowledge and understanding of issues related to Digital Safety and act on any areas of vulnerability.

To audit digital safety and the effectiveness of this policy, the following questions should be considered:

- Has recording of e-safety incidents been effective – are records kept?
- Did Halliford School feel able to respond effectively to any incidents?
- Were incidents resolved to the best of Halliford School's ability?
- Do all students demonstrate an awareness of e-safety appropriate to their age?
- Have complaints or concerns with the policy been recorded and addressed?
- Have there been significant developments in technology that should be addressed either within the curriculum or as part of staff awareness training?
- Is the policy clear to all staff and seen as appropriate and working?
- Is the current wording fit for purpose and reflective of technology use in Halliford School?
- Do all members of Halliford School community know how to report a problem?
- Is Digital Safety observed in teaching and present in curriculum planning documents?

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used for personal use during lessons or formal school time. Sixth Form students may use their mobile phones within the 6 th Form Common Room at lunchtime only.
- From time to time we understand that students may need to use mobile devices for learning and this must only be done with the permission of a teacher. If a student has their mobile phone confiscated, they will be asked to collect them from reception. Persistent offenders will be issued with a school detention and parents informed.
- The sending of abusive or inappropriate messages is forbidden.
- Where the use of a mobile phone in a restricted area or time is suspected, senior staff reserve the right to confiscate the phone and may require a search to be made, with appropriate supervision by a colleague, if harmful content or use is reasonably suspected. Both colleagues conducting a search must be female and will initially request permission from the student.

- The school considers carefully how to manage 3G, 4G and 5G accessibility – risk is managed by regular reminders to students, swift follow up to reported incidents, the locking of devices during the school day where required, the application of pastoral support or sanctions as required and close contact with parents and guardians.
- Staff will be issued with a school phone where contact with students is required, e.g. when taking school trips. Staff will not create WhatsApp groups with students.
- Any sanctions related to this are referenced in the school's Behaviour Policy.

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 students' electronic devices, including mobile phones, MS Gos 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 SMT 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*

** Staff may also confiscate devices for evidence to hand to the police, if a student discloses that they are being abused and that this abuse includes an online element.*

Any searching of students will be carried out in line with:

- The DfE's latest guidance Searching, screening and confiscation in schools - GOV.UK (www.gov.uk)
- Mobile phones in schools - GOV.UK (www.gov.uk)
- UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)

Appendix 1: Procedures for staff in the event of a breach of this policy by a student or adult

(A) An inappropriate website is accessed inadvertently:

- Report to DSL; and
- Contact ICT Support via email so that it can be added to the banned or restricted list.

(B) An inappropriate website is accessed deliberately:

- Ensure that no one else can access the material, by shutting down the computer;
- Record the incident in writing;
- Report to the DSL immediately; and
- The Deputy Head applies the Behaviour Policy.
- In serious cases the Headmaster should also be informed.

(C) An adult receives inappropriate material:

- Do not forward this material to anyone else – doing so could be an illegal activity;
- Alert the Headmaster immediately; and
- Ensure the device is shut down and record the nature of the material.

(D) An adult has used ICT equipment inappropriately:

- Follow the procedures for (B).

(E) An adult has communicated with a student, or used ICT equipment, inappropriately:

- Ensure the student is reassured;
- Report to the Headmaster who should follow the Safe Students Safe Staff Policy and Safeguarding and Child Protection Policy (if relevant);
- Preserve the information received by the student if possible, and determine whether the information received is abusive, threatening or innocent; and
- If illegal or inappropriate use is established, contact the Headmaster or Chair of Governors.

(F) Threatening or malicious comments are posted to Halliford School website or distributed via Halliford School email system (or printed out) about an adult in school:

- Preserve any evidence; and
- Inform the Headmaster immediately and follow the Safeguarding and Child Protection Policy as necessary.

(G) Where images of staff or adults are posted on inappropriate websites, or have inappropriate information about them posted anywhere:

- The Headmaster should be informed.

Appendix 2 – Student Acceptable User Policy (AUP)

Student Acceptable User Policy

Scope of this Policy

This policy applies to all students at Halliford School.

Online behaviour

As a member of the school community you should follow these principles in all of your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact students or parents, and students and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Using the school's IT systems and personal laptops

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems and laptop using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.

Passwords

Passwords protect the School's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

Use of Property

Any property belonging to the School should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to IT Support.

Use of school systems

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and students should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the school's right to monitor and access web history and email use.

Use of personal devices or accounts and working remotely

All official school business must be conducted on school systems, and it is not permissible to use personal email accounts for school business. Any use of personal devices such as laptops for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by IT Support.

Monitoring and access

Staff, parents and students should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

Any personal devices used by students, whether or not such use is permitted, may be confiscated and examined under such circumstances. Please refer to the mobile phone policy.

Compliance with related school policies

You will ensure that you comply with the school's Digital Safety, BYOD Protocols and other relevant policies, e.g. Safeguarding and Child Protection, Anti-Bullying, Behaviour.

Retention of digital data

All emails sent or received on school systems will be kept in archive. Important information that is necessary to be kept should be held on the relevant personnel or student file, not kept in personal folders, archives or inboxes. Hence it is the responsibility of each account user to ensure that important information is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the school's email deletion protocol.

If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact the Bursar. bursar@hallifordschool.co.uk

Breach reporting

The law requires the school to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, e.g. through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The school must generally report personal data breaches to the Information Commissioners Office (ICO) without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

Data breaches will happen to all organisations, but the school must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and students. The school's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

Breaches of this policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the school's usual procedures. In addition, a deliberate breach may result in the school restricting your access to school IT systems.

If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to the Designated Safeguarding Lead. Reports will be treated in confidence.

Acceptance of this policy

Please confirm that you understand and accept this policy by signing below and returning the signed copy to your form tutor.

I understand and accept this acceptable use policy:

Name: _____

Signature: _____

Date: _____

Parent / Guardian Signature (for students aged 11 – 16): _____

Appendix 3 – Staff, Governors and Volunteers Acceptable User Policy (AUP)

IT acceptable use policy

1 **Introduction:** This policy sets out the requirements with which you must comply when using the School's IT and when otherwise using IT in connection with your job including:

1.1 the School's email and internet services;

1.2 telephones

1.3 the use of mobile technology on School premises or otherwise in the course of your employment (including 4G / 5G or Bluetooth or other wireless technologies), whether using a School or a personal device; and

1.4 any hardware (such as laptops, printers or mobile phones) or software provided by, or made available by, the School.

This policy also applies to your use of IT off School premises if the use involves Personal Information of any member of the School community or where the culture or reputation of the School are put at risk.

2 **Failure to comply:** Failure to comply will constitute a disciplinary offence and will be dealt with under the School's disciplinary procedure.

3 **Property:** You should treat any property belonging to the School with respect and reasonable care and report any faults or breakages immediately to the Bursar. You should not use the School's computers or other IT resources unless you are competent to do so and should ask for training if you need it.

4 **Viruses and other malicious code:** You should be aware of the potential damage that can be caused by computer viruses and other malicious code. You must not use, introduce or operate any hardware, programmes or data (including computer games) or open suspicious emails without permission from the IT Support department.

5 **Passwords:** Passwords should be long, for example, you could use a song lyric or a memorable phrase plus a number. Do not choose a password which is so complex that it's difficult to remember without writing it down. Your password should not be disclosed to anyone else. In addition:

5.1 Your password should be difficult to guess, for example, you could base your password on something memorable that no-one else would know. You should not use information which other people might know, or be able to find out, such as your address or your birthday.

5.2 You must not use a password which is used for another account. For example, you must not use your password for your private email address or online services for any School account.

5.3 Passwords must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

6 **Leaving workstations:** If you leave your workstation for any period of time you should take appropriate action and, in particular, you should lock your screen to prevent access.

7 **Concerns**: You have a duty to report any concerns about the use of IT at the School to the Bursar. For example, if you have a concern about IT security or pupils accessing inappropriate material.

8 **Other policies**: This policy should be read alongside the following:

8.1 Code of Conduct;

8.2 Data Protection policy for Staff;

8.3 Acceptable Use Policy.

Internet

9 **Downloading:** Downloading of any programme or file which is not specifically related to your job is strictly prohibited.

10 **Personal use:** The School permits the incidental use of the internet so long as it is kept to a minimum and takes place substantially out of normal working hours. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. If the School discovers that excessive periods of time have been spent on the internet provided by the School or it has been used for inappropriate purposes (as described in section 11 below), either in or outside working hours, disciplinary action may be taken and internet access may be withdrawn without notice at the discretion of the Head.

11 **Unsuitable material:** Viewing, retrieving or downloading of pornographic, terrorist or extremist material, or any other material which the School believes is unsuitable is strictly prohibited and constitutes gross misconduct. This includes such use at any time on the School's network, or via 3G or 4G when on School premises or otherwise in the course of your employment and whether or not on a School or personal device. Internet access may be withdrawn without notice at the discretion of the Head whilst allegations of unsuitable use are investigated by the School.

12 **Location services**: The use of location services represents a risk to the personal safety of those within the School community, the School's security and its reputation. The use of any website or application, whether on a School or personal device, with the capability of publicly identifying the user's location while on School premises or otherwise in the course of employment is strictly prohibited at all times.

13 **Contracts:** You are not permitted to enter into any contract or subscription on the internet (including through an App) on behalf the School, without specific permission from the Bursar. This applies both to "free" and paid for contracts, subscriptions and Apps.

14 **Retention periods**: the School keeps a record of staff browsing histories for a period of 90 days.

Email

15 **Personal use:** The School permits the incidental use of its email systems to send personal emails as long as such use is kept to a minimum and takes place substantially out of normal working hours. Personal emails should be labelled "personal" in the subject header. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. The School may monitor your use of the email system, please see paragraphs 26-30 below, and staff should advise those they communicate with that such emails may be monitored. If the School discovers that you have breached these requirements, disciplinary action may be taken.

16 **Status:** Email should be treated in the same way as any other form of written communication. Anything that is written in an email is treated in the same way as any form of writing. You should not include anything in an email which is not appropriate to be published generally.

17 **Inappropriate use:** Any email message which is abusive, discriminatory on grounds of sex, marital or civil partnership status, age, race, disability, sexual orientation or religious belief (or otherwise contrary to our equal opportunities policy), or defamatory is not permitted. Use of the email system in this way constitutes gross misconduct. The School will take no responsibility for any offence caused by you as a result of downloading, viewing or forwarding inappropriate emails.

18 **Legal proceedings:** You should be aware that emails are disclosable as evidence in court proceedings and even if they are deleted, a copy may exist on a back-up system or other storage area.

19 **Jokes:** Trivial messages and jokes should not be sent or forwarded to the email system. They could cause the School's IT system to suffer delays and / or damage or could cause offence.

20 **Contracts:** Contractual commitments via an email correspondence are not allowed without the prior authorisation of the Bursar.

21 **Disclaimer:** All correspondence by email should contain the School's disclaimer.

22 **Data protection disclosures:** Subject to a number of limited exceptions, potentially all information about an individual may be disclosed should that individual make a subject access request under data protection legislation. There is no exemption for embarrassing information (for example, an exchange of emails containing gossip about the individual will usually be disclosable). **Staff must be aware that anything they put in an email is potentially disclosable.**

Monitoring

23 The School regularly monitors and accesses its IT system for purposes connected with the operation of the School. The School IT system includes any hardware, software, email account, computer, device or telephone provided by the School or used for School business. The School may / will also monitor staff use of the School telephone system and voicemail messages. Staff should be aware that the School ay / will monitor the contents of a communication (such as the contents of an email).

24 The purposes of such monitoring and accessing include:

24.1 to help the School with its day to day operations. For example, if a member of staff is on holiday or is off sick, their email account may / will be monitored in case any urgent emails are received; and

24.2 to check staff compliance with the School's policies and procedures and to help the School fulfil its legal obligations. For example, to investigate allegations that a member of staff has been using their email account to send abusive or inappropriate messages.

25 Monitoring may be carried out on a random basis and it may be carried out in response to a specific incident or concern.

26 The School also uses software which automatically monitors the School IT system (for example, it would raise an alert if a member of Staff visited a blocked website or sent an email containing an inappropriate word or phrase).

27 The monitoring is carried out by IT Support and Sensible IT Solutions. If anything of concern is revealed as a result of such monitoring then this information may be shared with the DSL and the Headmaster and this may result in disciplinary action. In exceptional circumstances concerns will need to be referred to external agencies such as the Police.

Acceptance of this policy

Please confirm that you understand and accept this policy by signing below and returning the signed copy to the Headmaster's PA.

I understand and accept this acceptable use policy:

Name: _____

Signature: _____

Date: _____

Appendix 4 – Bring Your Own Device Policy (BYOD) Staff & 6th Form Students only

Introduction

The school recognises that mobile technology offers valuable benefits to all from a teaching and learning perspective and to visitors. Our school embraces this technology but requires that it is used in an acceptable and responsible way.

This policy is intended to address the use by staff, students and visitors to the school of non-school owned electronic devices to access the internet via the school's internet connection, to access or store school information, or to make photographs, video, or audio recordings at school. These devices include smart phones, tablets, laptops, wearable technology and any similar devices. These devices are referred to as 'mobile devices' in this policy.

Sections one to three and five of this policy apply to all school staff and to visitors to the school. The rest of the policy is only relevant to school staff.

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.

1. Use of mobile devices at the school

Staff and students may use their own mobile devices in the following locations:

- In the classroom with the permission of the teacher
- In the school environment including Reception, Courtyard and Common Room and staff offices.

Visitors to the school are asked not to use their mobile devices at all unless in an area where they are away from students and supervised by a member of staff.

Staff and visitors to the school are responsible for their mobile device at all times. The school is not responsible for the loss or theft of or damage to the mobile device or storage media on the device (e.g. removable memory card) howsoever caused. Reception must be notified immediately of any damage, loss, or theft of a mobile device, and these incidents will be logged.

Mobile devices must be turned off when in a prohibited area and/or at a prohibited time and must not be taken into controlled assessments and/or examinations, unless special circumstances apply. The school reserves the right to refuse staff and visitors permission to use their own mobile devices on school premises.

2. Use of cameras and audio recording equipment

Parents and carers may take photographs, videos or audio recordings of their children at school events for their own personal use.

Other visitors and staff may use their own mobile devices to make photographs, video, or audio recordings in school provided they first obtain permission to take photographs, films or recordings of the relevant individuals. This includes people who might be identifiable in the background.

To respect everyone's privacy and in some cases protection, photographs, video, or audio recordings should not be published on blogs, social networking sites or in any other way without the permission of the people identifiable in them. Parents or carers should avoid commenting on activities involving students other than their own in photographs, video, or audio, and other visitors and staff should not comment.

No one must use mobile devices to record people at times when they do not expect to be recorded, and devices must not be used that would enable a third party acting remotely to take photographs, video, or audio recordings in school. Staff must comply with the school's Social Media guidance and Anti-Bullying policy when making photographs, videos, or audio recordings.

3. Access to the school's internet connection

The school provides a wireless network that staff, Sixth Form and visitors to the school may use to connect their mobile devices to the internet. Access to the wireless network is at the discretion of the school, and the school may withdraw access from anyone it considers is using the network inappropriately. To access the BYOD Wi-Fi connection.

Visitors – via a PW from SITS
Sixth Form via their MAC address supplied to SITS. Use of 2FA.

Staff via their Microsoft 365 access and using 2FA.

Staff may use the systems listed above to view school information via their mobile devices, including information about pupils. Staff must not store the information on their devices, or on cloud servers linked to their mobile devices.

Staff must only use the IT services listed above and any information accessed through them for work purposes. School information accessed through these services is confidential, in particular information about pupils. Staff must take all reasonable measures to prevent unauthorised access to it. Any unauthorised access to or distribution of confidential information should be reported to the school's IT team.

Staff must not send school information to their personal email accounts.

If in any doubt a device user should seek clarification and permission from the school's, IT team before attempting to gain access to a system for the first time.

The school is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the school's wireless network. This activity is taken at the owner's own risk and is discouraged by the school. The school will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the school's wireless network.

4. Access to school IT services

School staff are permitted to connect to or access the following school IT services from their mobile devices:

- the school email system;
- iSAMS

- MS Office

Staff may use the systems listed above to view school information via their mobile devices, including information about students. Staff must not store the information on their devices, or on cloud servers linked to their mobile devices. In some cases, it may be necessary for staff to download school information to their mobile devices in order to view it (for example, to view an email attachment). Staff must delete this information from their devices as soon as they have finished viewing it.

Staff must only use the IT services listed above and any information accessed through them for work purposes. School information accessed through these services is confidential, in particular information about students. Staff must take all reasonable measures to prevent unauthorised access to it. Any unauthorised access to or distribution of confidential information should be reported to the school's IT team.

Staff must not send school information to their personal email accounts.

If in any doubt a device user should seek clarification and permission from the school's, IT team before attempting to gain access to a system for the first time.

5. Monitoring the use of mobile devices

The school may use technology that detects and monitors the use of mobile and other electronic or communication devices which are connected to or logged on to our wireless network or IT systems. By using a mobile device on the school's IT network, staff and visitors to the school agree to such detection and monitoring. The school's use of such technology is for the purpose of ensuring the security of its IT systems and tracking school information.

The information that the school may monitor includes (but is not limited to): the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms (including passwords), information uploaded to or downloaded from websites and school IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

Staff who receive any inappropriate content through school IT services or the school internet connection should report this to the school's IT team as soon as possible.

6. Security of staff mobile devices

Staff must take all sensible measures to prevent unauthorised access to their mobile devices, including but not limited to the use of a PIN, pattern or password to be entered to unlock the device, and ensuring that the device auto-locks if inactive for a period of time.

Staff must never attempt to bypass any security controls in school systems or others' own devices.

Staff are reminded to familiarise themselves with the school's e-safety, social media and acceptable use of IT policies which set out in further detail the measures needed to ensure responsible behaviour online.

Staff must ensure that appropriate security software is installed on their mobile devices and must keep the software and security settings up-to-date.

Staff must only connect their personal devices to the BYOD network.

7. Compliance, Sanctions and Disciplinary Matters for staff

Non-compliance of this policy exposes both staff and the school to risks. If a breach of this policy occurs the school will respond immediately by issuing a verbal, then written warning to the staff member.
Guidance will also be offered. If steps are not taken by the individual to rectify the situation and adhere to the policy, then the mobile device in question may be confiscated and/or permission to use the device on school premises will be temporarily withdrawn. For persistent breach of this policy, the school will permanently withdraw permission to use user-owned devices in school.

8. Incidents and Response

The school takes any security incident involving a staff member's or visitor's personal device very seriously and will always investigate a reported incident. Loss or theft of the mobile device should be reported to Reception in the first instance. Data protection incidents should be reported immediately to the Bursar

Appendix 5 - Social Media Guidance

Social media is a broad term for any kind of online platform which enables people to directly interact with each other.

Halliford School recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by Halliford School, its staff, parents, carers and students.

Scope

This guidance is subject to the information contained in the Safe Students Safe Staff Policy and the Acceptable Use Agreements.

This policy:

- Applies to all staff and to all online communications which directly or indirectly represent Halliford School;
- Applies to such online communications posted at any time and from anywhere;
- Encourages the safe and responsible use of social media through training and education; and
- Defines the monitoring of public social media activity pertaining to Halliford School.

Halliford School respects privacy and understands that staff and students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or Halliford School's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using Halliford School name. All professional communications are within the scope of this policy. Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with Halliford School or impacts on Halliford School, it must be made clear that the member of staff is not communicating on behalf of Halliford School with an appropriate disclaimer. Such personal communications are within the scope of this guidance.

Personal communications which do not refer to or impact upon Halliford School are outside the scope of this guidance.

Digital communications with staff/students are also considered. Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes, but must consider whether this is appropriate and consider the potential implications.

Process for creating new accounts and monitoring use

Halliford School community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "friends of Halliford School" Facebook page. Anyone wishing to create such an account must present a case to the Headmaster which covers the following points:

- The aim of the account;
- The intended audience;
- How the account will be promoted;
- Who will run the account; and
- Will the account be open or private/closed.

Following consideration, an application will be approved or rejected. In all cases, the Headmaster must be satisfied that anyone running a social media account on behalf of Halliford School has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by Halliford School, including volunteers or parents.

School accounts must be monitored regularly and frequently to ensure appropriate use.

Appendix 6 - Social Media Do's and Don'ts

Managing your personal use of social media

- 'Nothing' on social media is truly private.
- Social media can blur the lines between your professional and private life. Don't use Halliford School logo and/or branding on personal accounts.
- Check your settings regularly and test your privacy.
- Keep an eye on your digital footprint.
- Keep your personal information private.
- Regularly review your connections – keep them to those you want to be connected to.
- When posting online, consider: scale, audience and permanency.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem.

The Do's:

- Check with a senior member of staff before publishing content that may have controversial implications for Halliford School;
- Use a disclaimer when expressing personal views;
- Make it clear who is posting content;
- Use an appropriate and professional tone;
- Be respectful to all parties;
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author;
- Express opinions but do so in a balanced and measured manner;
- Think before responding to comments and, when in doubt, get a second opinion;
- Seek advice and report any mistakes using Halliford School's reporting process; and
- Consider turning off tagging people in images where possible.

The Don'ts:

- Don't make comments, post content or link to materials that will bring Halliford School into disrepute;
- Don't publish confidential or commercially sensitive material;
- Don't breach copyright, data protection or other relevant legislation;
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content;
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content; and
- Don't use social media to air internal grievances.

Appendix 7 - Email etiquette

Email best practice

- Write well-structured emails and use short, descriptive subjects.
- Sentences can be short and to the point. You can start your email with 'Hi', or 'Dear', and the name of the person. The use of internet abbreviations and characters such as smileys is not encouraged.
- Signatures must include your name, job title and school name. A disclaimer should be added underneath your signature. This is automatically done on the Halliford School e-mail system.
- Users must spell check all mails prior to transmission.
- Only mark emails as important if they really are important.
- Avoid long strings of messages; start new conversations.

Do not

- Write it in an email unless you would put it on a noticeboard in the office or in a newspaper.
- Write anything that is libellous, defamatory, offensive, racist or obscene - you and Halliford School can be held liable.
- Forward confidential information - you and Halliford School can be held liable.
- Forward a message with sensitive information without acquiring permission from the sender first.
- Send email messages using another person's email account.

Appendix 8 - Microsoft Go Protocol

All students in Year 7 -11 have a Microsoft Go Device.

Full details regarding their use and how we develop Digital Skills within our students are covered within the Halliford School Digital Guide. An extract from this is contained below:

MS Go devices are an integral part of the curriculum at Halliford School. We are aware of the true benefits of a fully integrated approach to learning and how we can plan to maximise this potential in the future at Halliford. We are increasingly cognisant that we are part of an ever-changing world of technology and communication, and have over the course of the last few years invested heavily in the infrastructure required for ultra-fast broadband internet and all of our students will have access to this through our wireless system.

Making uniform the devices Halliford students use has allowed for consistency in planning, support and structure within our system, but also allows more readily for peer on peer problem solving, which is of real benefit. Halliford School wants to ensure that our students are prepared for the demands and opportunities of the digital age.

The aim pedagogically of this approach is to improve the learning environment for our students through the judicious use of technology where beneficial and appropriate. Measures will be taken to continue to develop the more traditional skills, such as hand writing. That said, we feel the increased use of technology reflects that of the wider world, and develops appropriate skills in our students for the future whilst also creating a significant positive impact on teaching and learning.

The use of the devices will vary somewhat between subjects and topics, with some lending themselves more or less to the use of technology. The devices will be seen very much as an enhancement and extension of the curriculum, with a blended approach very much maintained. As such devices in lessons are likely to be used in the following ways:

- Research through online sources, electronic textbooks, Teams or online learning platforms such as Doddle.
- Digital class and note books using One Note
- Annotating and writing text and mathematical equations on One Note
- Facilitating independence within lessons, whereby students can revisit slides and ideas at their
- own pace using the device
- Effective catch-up if absent, or re-learning of lessons, with homework, resources and lessons
- accessible through Teams
- Low stakes quizzing through online platforms such as Kerboodle, where immediate feedback can
- be provided
- Collaboration on projects, documents and tasks that enhance group work and sharing ofideas
- Creating multimedia presentations using a wealth of research, and software
- Recording and analysing practical work, such as in DT, PE, Science, Music and Drama
- Increasing the effectiveness of revision through immediate access to materials and self-testing applications.

The premise of the use of these devices is not to replace traditional methods and will be used alongside exercise books, hand-written work and more readily used teaching practises. We firmly believe that by pursuing this route, students will be able to engage in a wider range of activities in each lesson, have a more bespoke experience and one that facilitates learning and progress. Whilst the style of task may vary from traditional approaches, we fully expect student engagement to increase and thus the quality of output to do likewise.

Appendix 9 - Online Safety

Within the school online safety is taught through Computing, PSHE and assemblies. An outline of this is itemised below:

Computer Science

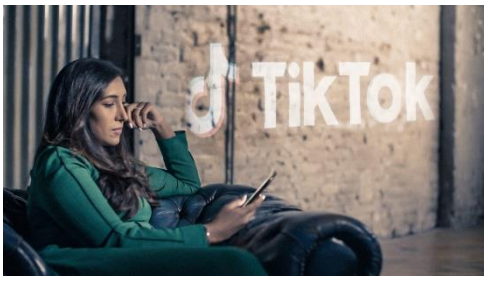
In Year 7 students are introduced to the e-safety acronym 'SMART'. This comprises five principles for staying safe online, including the idea that people may not be who they say they are, and 'don't meet up' with people you meet online.

In Year 8, students learn how to evaluate what they see online. They examine the harmfulness of online bullying and are taught to evaluate information that they read online for bias, subtext and hidden agendas. They examine the case studies of Jessie Nelson and Belle Gibson. They learn how and when to seek support.

In Year 9, student improve their abilities to evaluate what they see online, and learn to recognise techniques used for persuasion. They learn how social media can allow advertisers to circumvent legislation, how influencers may be deceptively selling, and how apps are designed to be sticky.

In Years 10 and 11, students taking GCSE study legislation and network security.

https://www.bbc.co.uk/iplayer/episode/m000p3p9/panorama-is-tiktok-safe



BBC iPlayer - Panorama - Is TikTok Safe?

Tina Daheley investigates whether TikTok, the social media sensation of lockdown, is safe for the millions of young people who have signed up.

www.bbc.co.uk

At A Level, privacy and data is on the syllabus, as is legislation.

Assemblies

In Headmaster's assemblies and House ones, online safety is addressed. The Safer Internet Day is celebrated each year and issues relating to online learning and safety have been covered.

Student E-Safety Forum

There is a prefect led E-Safety group who meet regularly to discuss the approaches we take as a school and to raise issues of good practice or concern within the school community.

PSHE

Year 7 - April-May June-July

Risk

With an ever growing online world, it is important to look at safety when using online platforms. Students develop safety techniques, what to do if something does not seem safe and how to protect yourself online. We also touch upon road safety and how to stay safe in certain circumstances.

Year 8 February-April

Your choice

It is important to understand that success and failure, morals and doing right or wrong is all down to the choices we make as individuals. We explore the idea of morals, decision making and the impact this has on individuals and others, both in person and online. We also look at how we can be influenced both positively and negatively.

Year 9 June-July

Staying Safe

Developing the topics covered in the year 7 unit 'risk' and the year 8 unit 'your choice', students will be looking at staying safe on the internet (who are you talking to), exploring the ways to stay safe when you are out and about, child protection and road safety.

Year 10 January-February

Staying Safe

Developing the unit from year 9, students will be exploring more elements of staying safe on line. Looking over your online profile, the do's and don'ts online. They will also explore safety at night, on the streets and how to deal with unsafe situations.

Staying safe within relationships.

Year 11 January - May

Students will understand diversity in sexual attraction. We will also address sex and relationship pressures that teenagers may encounter which includes elements such as sexting, pornography and the dark web. As well as developing student's awareness and knowledge of a range of sex and relationship issues and sexual health issues. Healthy and unhealthy relationships The aim of this unit

is for students to understand the importance of equality in relationships, the features of healthy and unhealthy relationships, that violence in relationships is unacceptable and to understand what support is available for those in an unhealthy relationship.

Diversity, discrimination, conflicting values and challenging offensive behaviour
Students will be exploring their own knowledge and understanding about diversity, discrimination and conflicting values and to develop strategies for challenging all forms of offensive behaviour including online bullying.

Guest Speakers

Screen Time – Aric Sigman

E-Safety – SWGfL

PSHE Drop Down Day, Wednesday 15 March 2023 – Delivered by Brook

7	8	9	10
Healthy Relationships	Healthy Relationships	Consent	Consent
Online Digital Life	Online Digital Life	Sexuality	Sexuality
Sexuality	Sexuality	Healthy Relationships	Healthy Relationships

Safer Internet Day

On Safer Internet Day, which is an annual event aimed at raising safety awareness, students receive an assembly on the topic of the year delivered by staff and students.

In addition, form tutors deliver a session to their forms as follows:

Year 7 – Sextortion and the dangers of sexting

Year 8 – Online behaviour and online bullying

Year 9 – The dangers of meeting up, grooming, identifying risks

Year 10 – How sexting can go wrong, identifying risks

Year 11 – Sextortion, identifying risk

Lower 6th – Sextortion, Sharing pictures online, Romance fraud, identifying risk

Upper 6th - Is social media addictive by design ? identifying risks

Appendix 10 – Summary of Compliance with – Meeting Digital and Technology Standard in School and Colleges 2022

Fibre.

- Leased 1GB/1GB Fibre Circuit in place
- /29 IP block to separate services
- Cloud based VOIP phone system in place
- VDSL backup/redundancy circuit in place
- Mirrored Routers in place
- Auto failover in place.

Servers

- Multiple Domain Controllers in different buildings
- Additional off site Domain Controllers
- DFS file replication in place for on-premise files in different buildings and off site
- UPS Protection in place on all key servers

Network Cabling

- All New building network is CAT6a compliant with relevant BS
- All New Building interconnect is Fibre with minimum 40GB bandwidth to OM4 specification with minimum 24 core

Network infrastructure

- Managed GB switches Bonded 'Star' Topology
- RST Spanning tree enabled an correctly configured on all switches
- All switches are POE+ , EEE to 802.3az
- Spare redundant switches are on site pre-configured
- No single 'CORE' single point of failure switch
- CCTV, VOIP, AP Management, Server Management all on separate VLANs
- UPS Protection in place on all key switches
- Firmware updates are automated on 'test' switches and if successful rolled out to other devices.

Wireless Network

- Cloud managed wireless network solution in place
- All AP's have 1GB back haul and support 2.4 and 5Ghz frequencies
- Rolling replacement of older devices to 802.11ax standard
- Monitored topology
- Sufficient APs to ensure 'blanket coverage' over the school site
- Spare APs ready to deploy in case of black spot or device failure
- Careful use of long and short range devices to ensure appropriate cover.
- Multiple SSIDs and AP groups separated by VLAN

General

- Senso Safeguarding in Place

Appendix 11 – Working Document for Compliance with Filtering and Monitoring Requirements in School – KCSIE 2023

REQUIREMENT FILTERING SYSTEM USED BY HALLIFORD SCHOOL – SENSO	➲
Is it a member of the Internet Watch Foundation (IWF)?	**Yes**
Is it signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)?	**Yes**
Does it block access to illegal content including child sexual abuse material (CSAM)?	**Yes**
Are you satisfied that the system manages the following content: › Discrimination › Drugs/substance abuse › Extremism › Gambling › Malware/hacking › Pornography › Piracy and copyright theft › Self harm › Violence	**Yes**

REQUIREMENT FILTERING SYSTEM USED BY HALLIFORD SCHOOL – SENSO	➲
Is the filtering system: › Operational › Up to date › Applied to all: o Users, including guest accounts o School-owned devices o Devices using the school broadband connection	Yes Yes – updated automatically. Applied to students and staff at Halliford School Applied all to school devices – MSGO Guests to use Halliford device to present (not bring in their own device)

REQUIREMENT FILTERING SYSTEM USED BY HALLIFORD SCHOOL – SENSO	➲
Does the filtering system: › Filter all internet feeds, including any backup connections. › Handle multilingual web content, images, common misspellings and abbreviations. › Identify technologies and techniques that allow users to get around the filtering, such as VPNs and proxy services, and block them It is worth noting that VPNs and Proxies are constantly evolving (on a daily basis), so filtering these is always a bit behind › Provide alerts when any web content has been blocked It is: › Age and ability appropriate for the users, and suitable for educational settings	Yes Yes Yes, industry standard. Yes Yes
Does the filtering system allow you to identify: › Device name or ID, IP address, and where possible, the individual › The time and date of attempted access › The search term or content being blocked	Yes Yes Yes

REQUIREMENT FILTERING SYSTEM USED BY HALLIFORD SCHOOL – SENSO	➲
Are you clear on how long logfile information (internet history) is retained and how it's stored?	Yes, stored on SENSO Chris Shier at Senso: *you have web logs as well as the violations which are kept for as long as the customer is in subscription with us.*
Are you clear on how the system does not over block access so it doesn't lead to unreasonable restrictions?	Yes

Does the filtering system meet the following principles? › Context appropriate differentiated filtering, based on age, vulnerability and risk of harm o Can you vary the filtering strength? E.g. for staff?	Yes – desktops different level to MSGO's
› Circumvention o Can you identify and manage technologies used to circumvent the system, e.g. virtual personal networks (VPNs), proxy services and domain name system (DNS) over Hypertext Transfer Protocol Secure (HTTPS). At the Network DNS Edge level HTTPS proxies and VPNS are blocked. Manual DNS entries such as 8.8.8.8 are blocked at the network edge forcing DNS to be known	Yes
› Control o Can you control the filter yourselves to permit or deny specific content?	Yes Yes
o Can you log any changes as part of an audit trail?	Yes
› Contextual content filters o In addition to URL or IP-based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked, this would include artificial intelligence (AI) generated content. For example, being able to contextually analyse text on a page and dynamically filter	SENSO to be checked
› Filtering Policy o Does your provider detail its approach to filtering, as well as over blocking? -	Yes
› Group/multi-site management o Can your system be deployed centrally, with a central policy and dashboard?	Yes
› Identification o Does the system allow you to identify users?	
› Multiple language support o Does the system manage relevant languages?	Chris Shier(Senso): Our filter module has sites in over 200 languages. For the keyword logging / monitoring in the safeguarding module,
› Network level o Is the filtering provided at 'network level', i.e. it doesn't rely on software on user devices while at school	

REQUIREMENT FILTERING SYSTEM USED BY HALLIFORD SCHOOL – SENSO	➲
	these keyword libraries built in are in English only. We have network filtering – Firewall and DNS but safeguarding is provided by SENSO which is a software install
› Remote devices ○ Can the system filter devices where staff and/or pupils are working remotely? › Reporting ○ Can you report inappropriate content? ○ Does the system provide clear historical information on the websites users have accessed or tried to access? › Safe Search ○ Does the system have the ability to enforce 'safe search'? -	Yes Yes Yes Yes
If users access content via mobile or through apps: Get confirmation that your provider can provide filtering on mobile or app technologies. They should also apply a technical monitoring system to devices using mobile and app content to reduce the risk of harm. › Students also do not have routine access to mobile phones during the day. However, there is no way of putting any software onto personal mobile devices.	SENSO – yes it is a key logger

REQUIREMENT FILTERING SYSTEM USED BY HALLIFORD SCHOOL – SENSO	➲
If your filtering provision is procured with a broadband service: Make sure it meets the needs of your school or college	No

REQUIREMENT MONITORING SYSTEM – SENSO	➲
Are incidents urgently picked up, acted on and the outcomes recorded? DSL HM and Bursar	Yes, via alerts from Senso
Are all staff clear on: › How to deal with these incidents › Who should lead on any actions	Yes but will clarify again at INSET DSL should lead on this
Is device monitoring managed? (this could be by your IT staff or a third-party provider) Whoever is manging device monitoring will need to: › Make sure monitoring systems are working as expected SITS › Provide reports on pupil device activity HF through Senso › Receive safeguarding training including online safety HF › Record and report safeguarding concerns to the DSL - Both	Managed by DSL, HM & SITS

REQUIREMENT MONITORING SYSTEM – SENSO	➲
Is your monitoring data received in a format that your staff can understand?	Need to look at reports from SENSO as very clunky and difficult to use for Governors etcTesting Seculy.
Are users identifiable to your school or college, so you can trace concerns to an individual, including guest accounts?	If we use Securly SmartDNS with a proxy PC then we can allow BYOD as they will use their 365 account to login – and can then be traced – this is for filtering NOT safeguarding

REQUIREMENT MONITORING SYSTEM – SENSO	➲
Does your monitoring system alert you to behaviours associated with: › Content o Being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism	Yes – key logging.
› Contact o Being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes	Yes – key logging.
› Conduct o Online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying	Yes – key logging.
› Commerce o Risks such as online gambling, inappropriate advertising, phishing and/or financial scams	Yes – gambling is blocked.

Does the monitoring system meet the following principles: › Age appropriate o Can you vary your strategy to take age, vulnerability, or specific situations (e.g. boarding schools) into account › Audit trail o Are any changes to the strategy logged so no one can make changes on their own? › Bring your own device (BYOD) o If your system can monitor staff and pupils' personal devices, make sure this is done according to your data management policies. For example, will your system monitor devices out of school hours? › Data retention o Be clear on what data is stored, where and for how long (including any backup data) › Devices o Make sure your system is clear about which devices it covers › Flexibility o Make it clear how keywords can be added or removed › Group/multi-site management o Can your strategy be deployed centrally, with a central policy and dashboard? › Harmful image detection o To what extent is visual content monitored and analysed? › Impact o How do monitoring results impact your policy and practice?	Yes Yes There is no BYOD policy. As long as there is an active license Yes – documented here Yes – controlled / advised by IWF. Can whitelist if needed Yes We are testing Seculy Any significant trends and patterns are identified and discussed by the DSL Team.

REQUIREMENT MONITORING SYSTEM – SENSO	➲
› Monitoring policy o How do you tell all users that you're monitoring their online access? o How do you communicate your expectations on appropriate use to pupils and staff? › Multiple language support o Can the system manage relevant languages to your school? › Prioritisation o How are alerts prioritised? o What procedures do you have in place to allow staff to respond to alerts rapidly? › Remote monitoring o Can the system monitor devices where staff and/or pupils are working remotely? o Are users aware of this? Are you clear if these devices are only monitored during school hours? › Reporting o How are alerts recorded, communicated and escalated?	Added to the staff AUP. AUP and INSET Training for Staff and Assemblies for students. Yes Alerts prioritised – Low / Medium / High grading in SENSO Emailed to DSLand HM inbox. Yes as long as on school device
Do your staff: › Provide effective supervision › Take steps to maintain awareness of how devices are being used by pupils › Report any safeguarding concerns to the DSL	Yes, but will clarify roles and responsibilities again at INSET

REQUIREMENT MONITORING SYSTEM – SENSO	➲
If users access content via mobile or through apps: Have you applied a technical monitoring system to these devices?	Yes on school devices but not mobile phones as not possible.